Groups and Symmetries

F. Oggier & A. M. Bruckstein

Division of Mathematical Sciences, Nanyang Technological University,
Singapore

These notes were designed to fit the syllabus of the course "Groups and Symmetries", taught at Nanyang Technological University in autumn 2012, and 2013.

Many thanks to Dr. Nadya Markin and Fuchun Lin for reading these notes, finding things to be fixed, proposing improvements and extra exercises. Many thanks as well to Yiwei Huang who got the thankless job of providing a first latex version of these notes.

These notes went through several stages: handwritten lecture notes (later on typed by Yiwei), slides, and finally the current version that incorporates both slides and a cleaned version of the lecture notes. Though the current version should be pretty stable, it might still contain (hopefully rare) typos and inaccuracies.

Relevant references for this class are the notes of K. Conrad on planar isometries [3, 4], the books by D. Farmer [5] and M. Armstrong [2] on groups and symmetries, the book by J. Gallian [6] on abstract algebra. More on solitaire games and palindromes may be found respectively in [1] and [7].

The images used were properly referenced in the slides given to the students, though not all the references are appearing here. These images were used uniquely for pedagogical purposes.

Contents

1 Isometries of the Plane 5

2 Symmetries of Shapes 25

3 Introducing Groups 41

4 The Group Zoo 69

5 More Group Structures 93

6 Back to Geometry 123

7 Permutation Groups 147

8 Cayley Theorem and Puzzles 171

9 Quotient Groups 191

10 Infinite Groups 211

11 Frieze Groups 229

12 Revision Exercises 253

13 Solutions to the Exercises 255

Chapter 1

Isometries of the Plane

> *"For geometry, you know, is the gate of science, and the gate is so low and small that one can only enter it as a little child."* (W. K. Clifford)

The focus of this first chapter is the 2-dimensional real plane $\mathbb{R}^2$, in which a point P can be described by its coordinates:

$$P \in \mathbb{R}^2,\ P = (x, y),\ x \in \mathbb{R},\ y \in \mathbb{R}.$$

Alternatively, we can describe P as a complex number by writing

$$P = (x, y) = x + iy \in \mathbb{C}.$$

The plane $\mathbb{R}^2$ comes with a usual distance. If $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in \mathbb{R}^2$ are two points in the plane, then

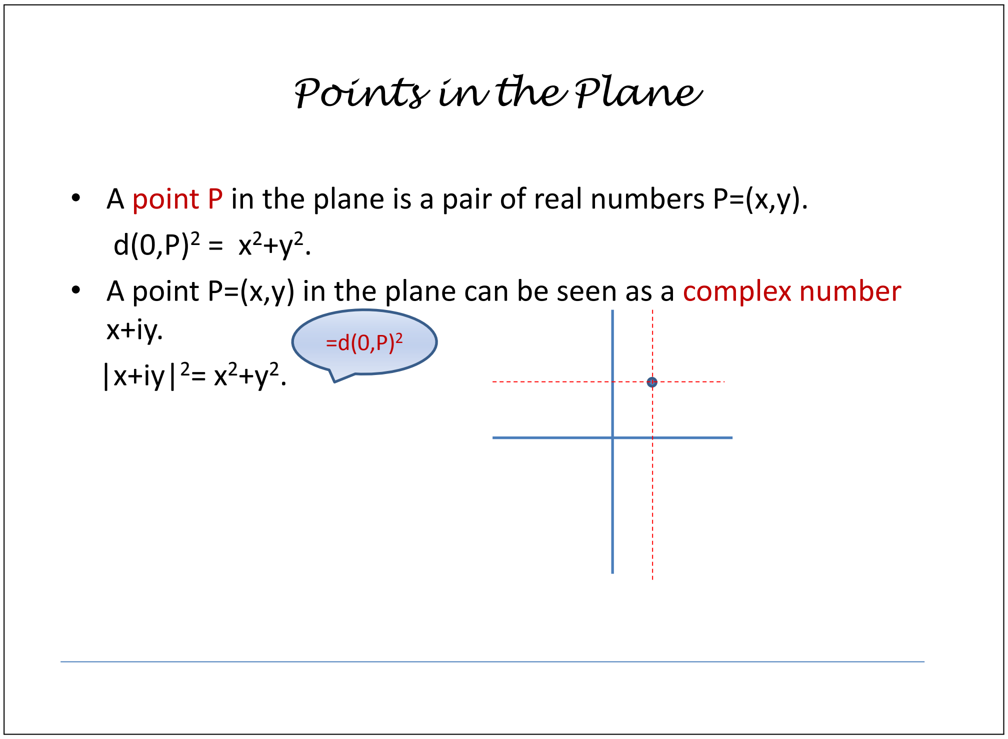
$$d(P_1, P_2) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Note that this is consistent with the complex notation. For $P = x + iy \in \mathbb{C}$, recall that $|P| = \sqrt{x^2 + y^2} = \sqrt{P\overline{P}}$, thus for two complex points $P_1 = x_1 + iy_1,\ P_2 = x_2 + iy_2 \in \mathbb{C}$, we have

$$\begin{aligned} d(P_1, P_2) &= |P_2 - P_1| = \sqrt{(P_2 - P_1)\overline{(P_2 - P_1)}} \\ &= |(x_2 - x_1) + i(y_2 - y_1)| = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}, \end{aligned}$$

where $\overline{(\ )}$ denotes the complex conjugation, i.e. $\overline{x + iy} = x - iy$.

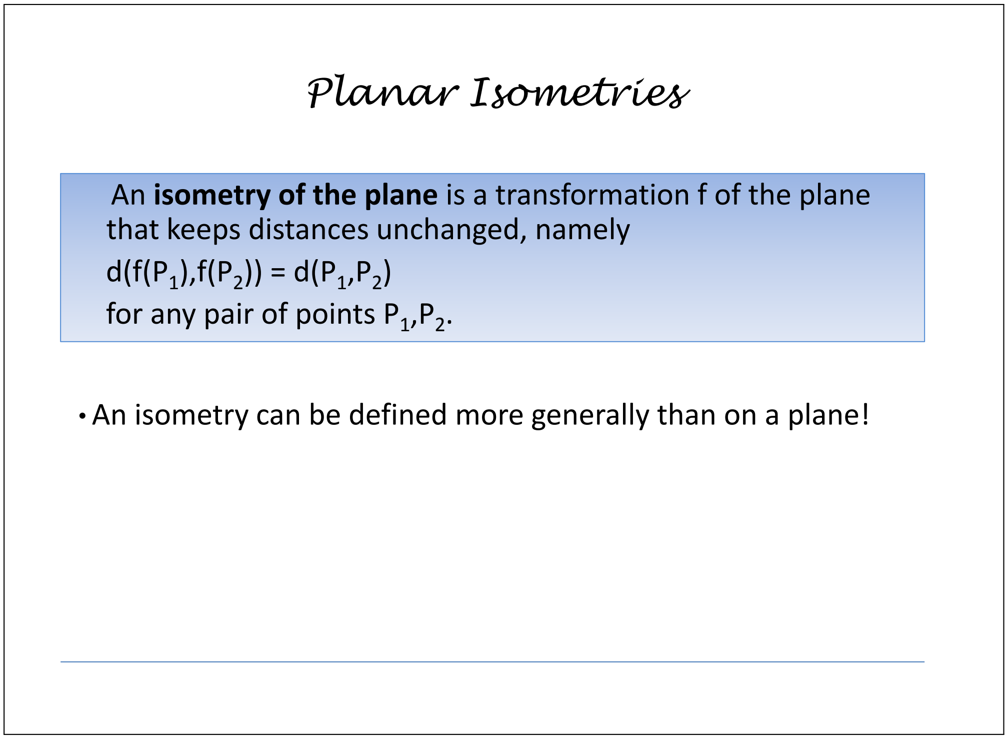
We are now interested in planar transformations (that is, maps from $\mathbb{R}^2$ to $\mathbb{R}^2$) that preserve distances.



Points in the Plane

- A point P in the plane is a pair of real numbers P=(x,y).
  $d(0,P)^2 = x^2+y^2$.
- A point P=(x,y) in the plane can be seen as a complex number x+iy.
  $|x+iy|^2 = x^2+y^2$.

$=d(0,P)^2$



Planar Isometries

An **isometry of the plane** is a transformation f of the plane that keeps distances unchanged, namely
$d(f(P_1),f(P_2)) = d(P_1,P_2)$
for any pair of points P_1,P_2.

- An isometry can be defined more generally than on a plane!

Definition 1. A map φ from $\mathbb{R}^2$ to $\mathbb{R}^2$ which preserves the distance between points is called a planar isometry. We write that

$$d(\varphi(P_1), \varphi(P_2)) = d(P_1, P_2)$$

for any two points P_1 and P_2 in $\mathbb{R}^2$.

What are examples of such planar isometries?

1. Of course, the most simple example is the identity map! Formally, we write
$$(x, y) \mapsto (x, y)$$
for every point $P = (x, y)$ in the plane.
2. We have the reflection with respect to the x-axis:
$$(x, y) \mapsto (-x, y).$$
3. Similarly, the reflection can be done with respect to the y-axis:
$$(x, y) \mapsto (x, -y).$$
4. Another example that easily comes to mind is a rotation.

Let us recall how a rotation is defined. A rotation counterclockwise through an angle θ about the origin $(0, 0) \in \mathbb{R}^2$ is given by

$$(x, y) \mapsto (x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta).$$

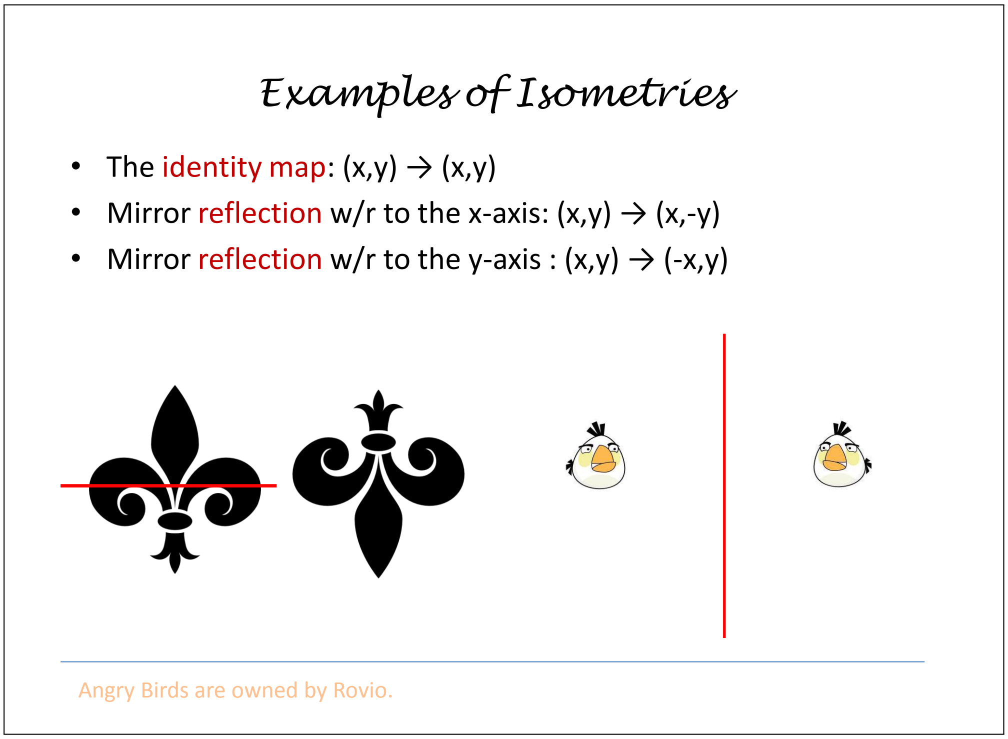
This can be seen using complex numbers. We have that $|e^{i\theta}| = 1$, for $\theta \in \mathbb{R}$, thus

$$|(x + iy)e^{i\theta}| = |x + iy|$$

and multiplying by $e^{i\theta}$ does not change the length of (x, y). Now

$$\begin{aligned} (x + iy)e^{i\theta} &= (x + iy)(\cos\theta + i \sin\theta) \\ &= (x \cos\theta - y \sin\theta) + i(x \sin\theta + y \cos\theta) \end{aligned}$$

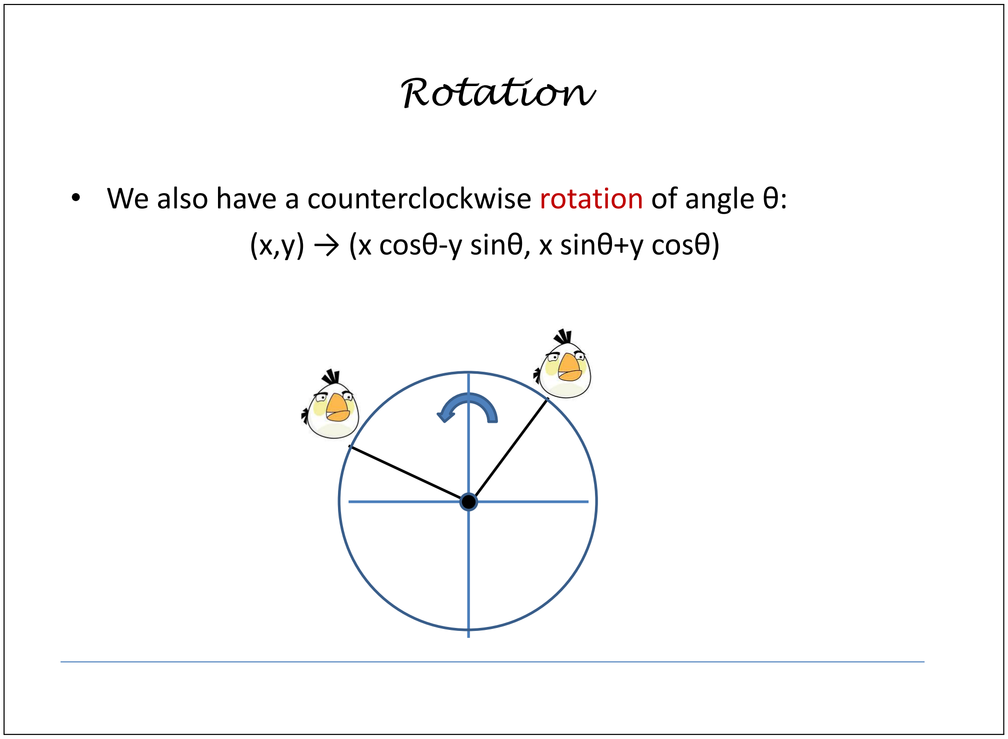
which is exactly the point $(x \cos\theta - y \sin\theta, x \sin\theta + y \cos\theta)$.



Examples of Isometries

- The identity map: (x,y) → (x,y)
- Mirror reflection w/r to the x-axis: (x,y) → (x,-y)
- Mirror reflection w/r to the y-axis : (x,y) → (-x,y)

Angry Birds are owned by Rovio.



Rotation

- We also have a counterclockwise rotation of angle θ:

  (x,y) → (x cosθ-y sinθ, x sinθ+y cosθ)

In matrix notation, a rotation counterclockwise through an angle θ about the origin $(0,0) \in \mathbb{R}^2$ maps a point $P = (x,y)$ to $P' = (x',y')$, where $P' = (x',y')$ is given by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}. \tag{1.1}$$

We denote the rotation matrix by R_θ:

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Intuitively, we know that a rotation preserve distances. However, as a warm-up, let us prove that formally. We will give two proofs: one in the 2-dimensional real plane, and one using the complex plane.

First proof. Suppose we have two points $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2) \in \mathbb{R}^2$. Let $d(P_1, P_2)$ be the distance from P_1 to P_2, so that the square distance $d(P_1, P_2)^2$ can be written as

$$\begin{aligned} d(P_1,P_2)^2 &= (x_2-x_1)^2 + (y_2-y_1)^2 \\ &= (x_2-x_1, y_2-y_1) \begin{bmatrix} x_2-x_1 \\ y_2-y_1 \end{bmatrix} \\ &= \left(\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} - \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \right)^T \left(\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} - \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \right), \end{aligned}$$

where $()^T$ denotes the transpose of a matrix.

Now we map two points P_1, P_2 to P_1' and P_2' via (1.1), i.e.

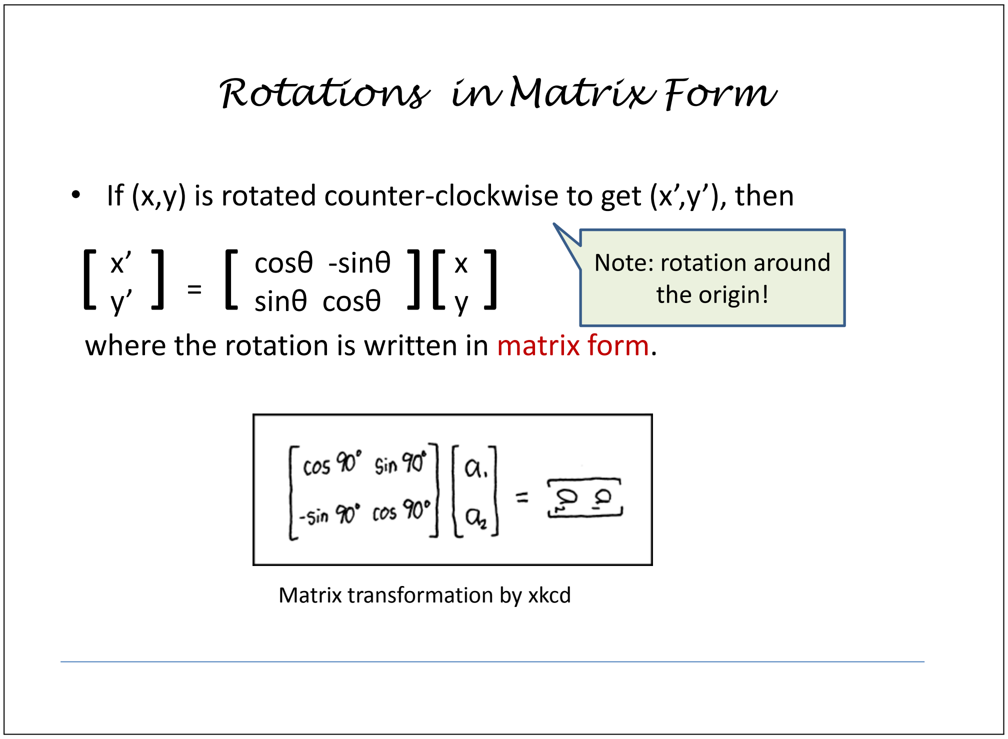
$$\begin{bmatrix} x_i' \\ y_i' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} = R_\theta \begin{bmatrix} x_i \\ y_i \end{bmatrix},\ i = 1,2.$$

Hence we have

$$\begin{bmatrix} x_2' \\ y_2' \end{bmatrix} - \begin{bmatrix} x_1' \\ y_1' \end{bmatrix} = R_\theta \left(\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} - \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \right),$$

and

$$\begin{aligned} d(P_1',P_2')^2 &= \left(\begin{bmatrix} x_2' \\ y_2' \end{bmatrix} - \begin{bmatrix} x_1' \\ y_1' \end{bmatrix} \right)^T \left(\begin{bmatrix} x_2' \\ y_2' \end{bmatrix} - \begin{bmatrix} x_1' \\ y_1' \end{bmatrix} \right) \\ &= \left(\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} - \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \right)^T R_\theta^T R_\theta \left(\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} - \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \right). \end{aligned}$$



cos 90° sin 90°
-sin 90° cos 90°
a1
a2
=

Rotations in Matrix Form

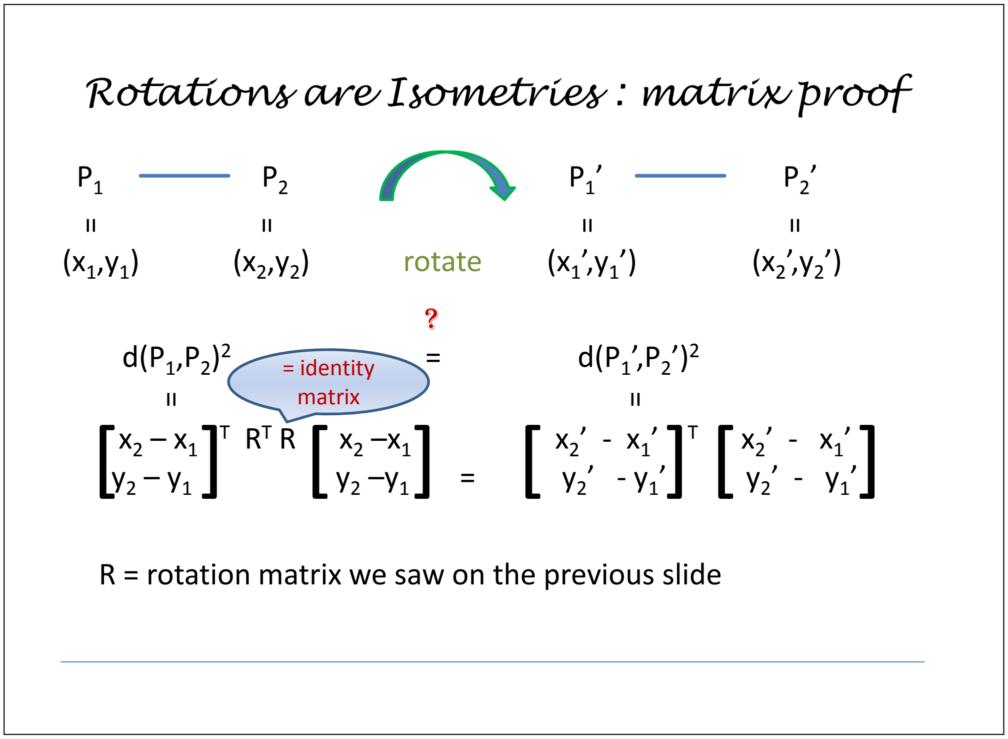
- If (x,y) is rotated counter-clockwise to get (x',y'), then

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Note: rotation around the origin!

where the rotation is written in matrix form.

Matrix transformation by xkcd



Rotations are Isometries : matrix proof

P_1 — P_2 rotate P_1' — P_2'

$P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2)$, $P_1' = (x_1',y_1')$, $P_2' = (x_2',y_2')$

$$d(P_1,P_2)^2 \overset{?}{=} d(P_1',P_2')^2$$

= identity matrix

$$\begin{bmatrix} x_2 - x_1 \\ y_2 - y_1 \end{bmatrix}^T R^T R \begin{bmatrix} x_2 - x_1 \\ y_2 - y_1 \end{bmatrix} = \begin{bmatrix} x_2' - x_1' \\ y_2' - y_1' \end{bmatrix}^T \begin{bmatrix} x_2' - x_1' \\ y_2' - y_1' \end{bmatrix}$$

R = rotation matrix we saw on the previous slide

But

$$R_\theta^T R_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

which establishes that $d(P_1', P_2') = d(P_1, P_2)$.

Second proof. Let $P_1 = x_1 + iy_1,\ P_2 = x_2 + iy_2$ be two points in $\mathbb{C}$, with distance

$$d(P_1, P_2) = |P_2 - P_1| = \sqrt{(P_2 - P_1)\overline{(P_2 - P_1)}}.$$

Since a rotation of angle θ about the origin is represented by a multiplication by $e^{i\theta}$, we have

$$\begin{aligned} d(P_1', P_2') &= |P_2' - P_1'| = \left|e^{i\theta}P_2 - e^{i\theta}P_1\right| = \left|e^{i\theta}(P_2 - P_1)\right| \\ &= \left|e^{i\theta}\right| |P_2 - P_1| = |P_2 - P_1| = d(P_1, P_2). \end{aligned}$$

An arbitrary planar transformation maps $P = (x, y)$ to $P' = (\varphi(x, y), \psi(x, y))$, or in complex notation, $P = x + iy$ to $P' = \varphi(x, y) + i\psi(x, y) = H(P)$.

We are interested in special planar transformations, those which preserve distances, called isometries. We gave a few examples of planar isometries, we will next completely classify them.

To do so, we will work with the complex plane, and write an isometry as $H(z),\ z \in \mathbb{C}$, such that

$$|z_1 - z_2| = |H(z_1) - H(z_2)|.$$

We shall show that

Theorem 1. *If $|H(z_1) - H(z_2)| = |z_1 - z_2|$, for all $z_1, z_2 \in \mathbb{C}$, then $H(z) = \alpha z + \beta$ or $H(z) = \alpha\overline{z} + \beta$ with $|z| = 1$, i.e. $\alpha = e^{i\theta}$ for some θ.*

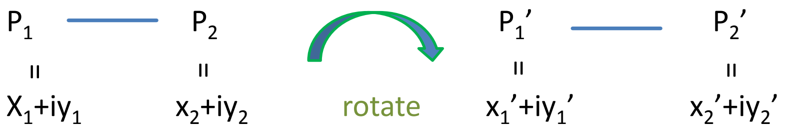
The theorem says that any function that preserves distances in $\mathbb{R}^2$ must be of the form

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} t_x \\ t_y \end{bmatrix}$$

or

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} t_x \\ t_y \end{bmatrix}.$$

Rotations are Isometries: complex proof



$$\begin{array}{ccccc} P_1 & P_2 & & P_1' & P_2' \\ \shortparallel & \shortparallel & & \shortparallel & \shortparallel \\ X_1+iy_1 & x_2+iy_2 & \text{rotate} & x_1'+iy_1' & x_2'+iy_2' \end{array}$$

$$\begin{array}{ccc} d(P_1,P_2) & \overset{?}{=} & d(P_1',P_2') \\ \shortparallel & & \shortparallel \\ |P_2-P_1| & = & |e^{\theta i}P_2-e^{\theta i}P_1| \\ & & \shortparallel \\ & & |e^{\theta i}|\ |P_2-P_1| \end{array}$$

Classification of Isometries of the plane

- Consider an arbitrary planar transformation map H, which maps a point P=x+iy to H(P).
- We are interested in classifying the maps H which are isometries, that is maps H satisfying $|H(z_1)-H(z_2)|=|z_1-z_2|$.

Notice what we recognize the reflections with respect to both the x- and y-axis, rotations around the origin, as well as translations.

In order to prove the theorem, we need the following cute lemma.

Lemma 1. *An isometry which maps* $(0,0)$ *to* $(0,0)$, $(1,0)$ *to* $(1,0)$*, and* $(0,1)$ *to* $(0,1)$, *i.e. (*0 *to* $0 \in \mathbb{C}$, 1 *to* $1 \in \mathbb{C}$, *and* i *to* $i \in \mathbb{C}$) *must be the identity map* $(x,y) \to (x,y)$.

Proof. The proof is done by identifying $\mathbb{R}^2$ with the complex plane. Let $h(z)$ be a planar isometry satisfying the assumptions of the lemma, in particular, $h(z)$ satisfies

$$|h(z_1) - h(z_2)| = |z_1 - z_2| \ \forall z_1, z_2 \in \mathbb{C}.$$

We then have

$$|h(z) - h(0)| = |z - 0|,$$

also

$$|h(z) - h(0)| = |h(z) - 0|$$

by assumption that $h(0) = 0$, thus

$$|h(z) - h(0)| = |h(z) - 0| = |z - 0|.$$

Using the fact that

$$h(1) = 1, \ h(i) = i,$$

we similarly get

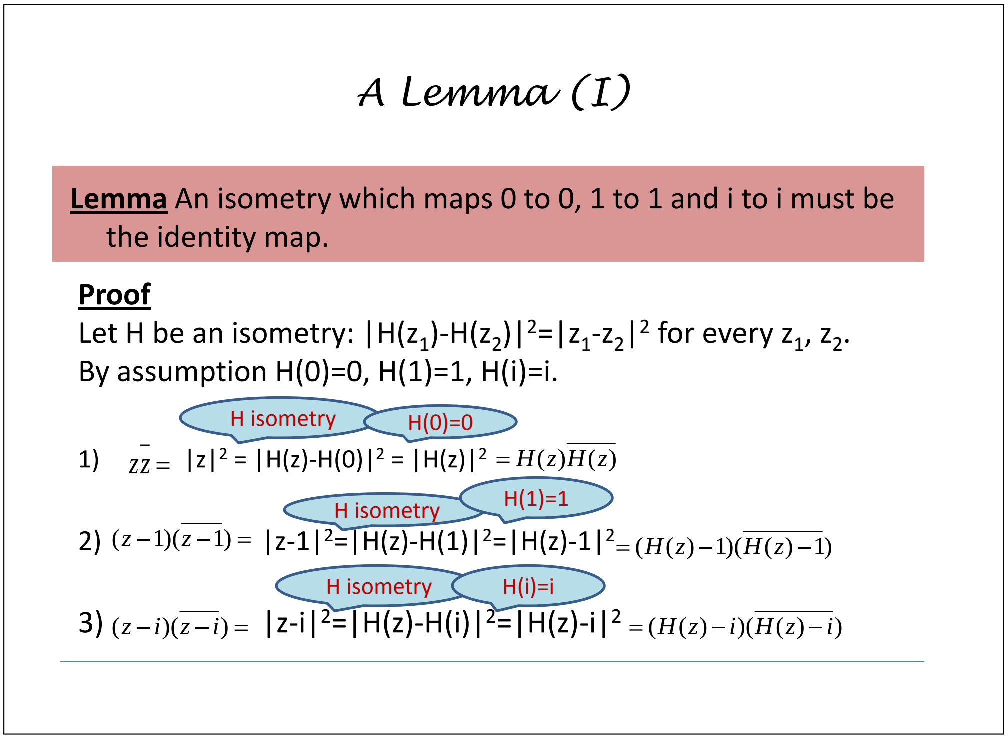
$$\begin{aligned}
|h(z) - 0| &= |h(z)| = |z - 0| = |h| \\
|h(z) - h(1)| &= |h(z) - 1| = |z - 1| \\
|h(z) - h(i)| &= |h(z) - i| = |z - i| \,.
\end{aligned}$$

This shows that

$$\begin{aligned}
&h(z)\overline{h(z)} = z\overline{z} \\
&(h(z) - 1)(\overline{h(z) - 1}) = (z - 1)\overline{(z - 1)} \\
&(h(z) - i)\overline{(h(z) - i)} = (z - i)\overline{(z - i)}.
\end{aligned}$$

We now multiply out

$$(h(z)-1)(\overline{h(z) - 1}) = h(z)\overline{h(z)} - h(z) - \overline{h(z)} + 1 = (z-1)\overline{(z - 1)} = z\bar{z} - z - \bar{z} + 1,$$



A Lemma (I)

Lemma An isometry which maps 0 to 0, 1 to 1 and i to i must be the identity map.

Proof

Let H be an isometry: $|H(z_1)-H(z_2)|^2=|z_1-z_2|^2$ for every z_1, z_2.

By assumption H(0)=0, H(1)=1, H(i)=i.

H isometry

H(0)=0

1) $z\bar{z} = |z|^2 = |H(z)-H(0)|^2 = |H(z)|^2 = H(z)\overline{H(z)}$

H isometry

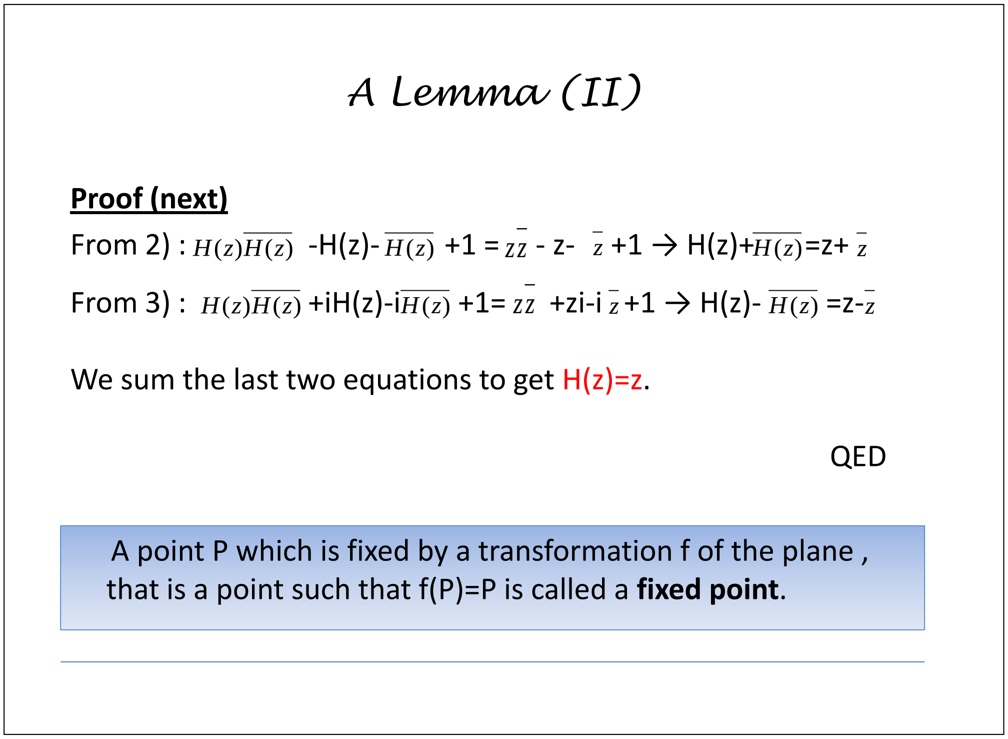
H(1)=1

2) $(z-1)\overline{(z-1)} = |z-1|^2=|H(z)-H(1)|^2=|H(z)-1|^2= (H(z)-1)\overline{(H(z)-1)}$

H isometry

H(i)=i

3) $(z-i)\overline{(z-i)} = |z-i|^2=|H(z)-H(i)|^2=|H(z)-i|^2 = (H(z)-i)\overline{(H(z)-i)}$



A Lemma (II)

Proof (next)

From 2) : $H(z)\overline{H(z)}$ $-H(z)-\overline{H(z)}+1 = z\bar{z} - z - \bar{z} + 1 \rightarrow H(z)+\overline{H(z)}=z+\bar{z}$

From 3) : $H(z)\overline{H(z)}+iH(z)-i\overline{H(z)}+1= z\bar{z} +zi-i\bar{z}+1 \rightarrow H(z)-\overline{H(z)}=z-\bar{z}$

We sum the last two equations to get H(z)=z.

QED

A point P which is fixed by a transformation f of the plane , that is a point such that f(P)=P is called a **fixed point**.

which can be simplified using that $h(z)\overline{h(z)} = z\overline{z}$, and similarly multiplying out $(h(z)-i)\overline{(h(z)-i)} = (z-i)\overline{(z-i)}$, we obtain

$$\begin{aligned} h(z)+\overline{h(z)} &= z+\overline{z} \\ h(z)-\overline{h(z)} &= z-\overline{z}. \end{aligned}$$

By summing both equations, we conclude that $h(z) = z$. □

In words, we have shown that if $h(z)$ has the same distances to $0, 1, i$ as z then $h(z)$ and z must be the same. This technique of looking at points which are fixed by a given planar transformation is useful and we will see it again later. It is thus worth giving a name to these special fixed points.

Definition 2. Let φ be a planar transformation. Then a point P in the plane such that $\varphi(P) = P$ is called a fixed point of φ.

We are now ready to classify planar isometries, that is to prove Theorem 1.

Proof. Given $H(z)$, an isometry $H : \mathbb{C} \to \mathbb{C}$, define

$$\begin{aligned} \beta &= H(0), \\ \alpha &= H(1)-H(0) \\ (|\alpha| &= |H(1)-H(0)| = |1-0| = 1). \end{aligned}$$

Now consider a new function

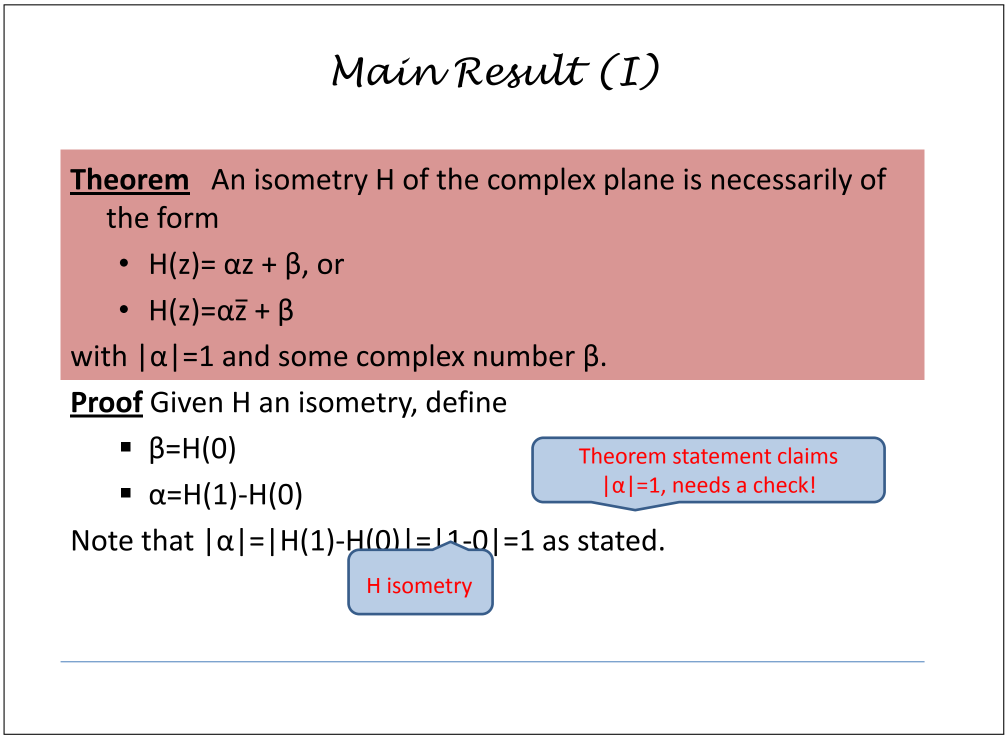
$$K(z) = \frac{H(z)-H(0)}{H(1)-H(0)} = \alpha^{-1}(H(z)-\beta).$$

Note the denominator is non-zero! Claim: $K(z)$ is also an isometry. Indeed, for every $z, w \in \mathbb{C}$, we have

$$\begin{aligned} |K(z)-K(w)| &= \left|\frac{H(z)-\beta}{\alpha} - \frac{H(w)-\beta}{\alpha}\right| \\ &= \left|\frac{H(z)-H(w)}{\alpha}\right| = \frac{|H(z)-H(w)|}{|\alpha|} \\ &= |H(z)-H(w)| = |z-w|\,. \end{aligned}$$

Now

$$\begin{aligned} K(0) &= \frac{H(0)-H(0)}{H(1)-H(0)} = 0 \\ K(1) &= \frac{H(1)-H(0)}{H(1)-H(0)} = 1. \end{aligned}$$



Main Result (I)

Theorem An isometry H of the complex plane is necessarily of the form

- $H(z)= \alpha z + \beta$, or
- $H(z)=\alpha\bar{z} + \beta$

with $|\alpha|=1$ and some complex number β.

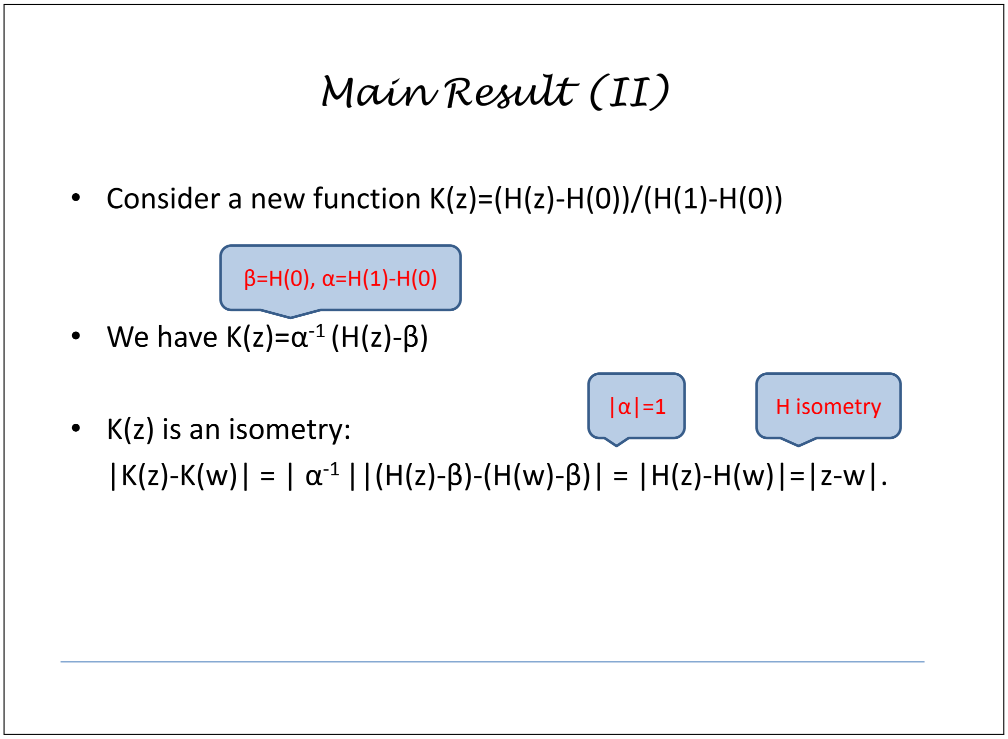
Proof Given H an isometry, define

- $\beta=H(0)$
- $\alpha=H(1)-H(0)$

Theorem statement claims $|\alpha|=1$, needs a check!

Note that $|\alpha|=|H(1)-H(0)|=|1-0|=1$ as stated.

H isometry



Main Result (II)

- Consider a new function $K(z)=(H(z)-H(0))/(H(1)-H(0))$

$\beta=H(0)$, $\alpha=H(1)-H(0)$

- We have $K(z)=\alpha^{-1}(H(z)-\beta)$

$|\alpha|=1$ H isometry

- K(z) is an isometry:
  $|K(z)-K(w)| = |\alpha^{-1}||(H(z)-\beta)-(H(w)-\beta)| = |H(z)-H(w)|=|z-w|$.

Then

$$\begin{aligned} |K(i)| &= |i| = 1 \\ |K(i)-1| &= |i-1| = \sqrt{2}. \end{aligned}$$

These two equations tell us that $K(i)$ is either i or $-i$. This can be seen from a geometric point of view, by noticing that $K(i)$ is both on the unit circle around the origin 0 and on a circle of radius $\sqrt{2}$ around 1. Alternatively, multiplying out $(K(i)-1)\overline{(K(i)-1)} = 2$ and simplifying the expression obtained with $K(i)\overline{K(i)} = 1$ leads to the same conclusion.

If $K(i) = i$, then by Lemma 1, we have that

$$K(z) = z \Rightarrow H(z) = \alpha z + \beta.$$

If instead $K(i) = -i$, then $\overline{K(z)}$ is an isometry that fixes $0, 1, i$ hence

$$\overline{K(z)} = z \Rightarrow K(z) = \overline{z},\ \forall z \in \mathbb{C},$$

and in this case

$$H(z) = \alpha\overline{z} + \beta.$$

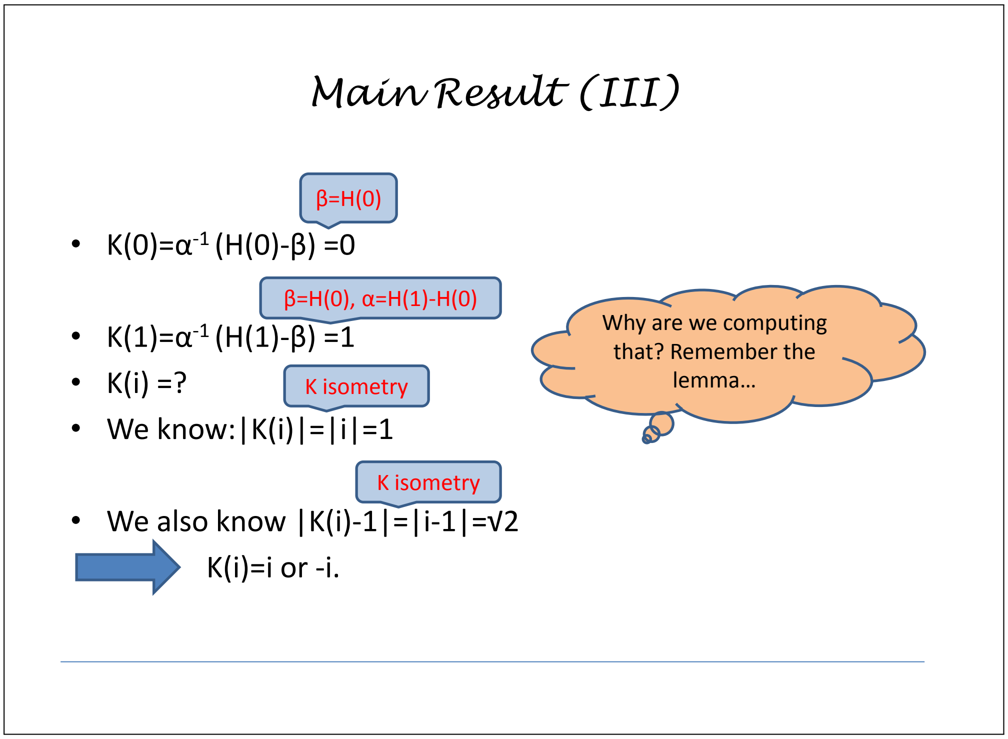
□

Let us stare at the statement of the theorem we just proved for a little bit. It says that every planar isometry has a particular form, and we can recognize some of the planar isometries that come to our mind (rotations around the origin, reflections around either the x- and y-axis, translations,...). But then, since we cannot think of other transformations, does it mean that no other exists? One can in fact prove the following:

Theorem 2. *Any planar isometry is either*

1. *a pure translation,*
2. *a pure rotation about some center z_0,*
3. *a reflection about a general line,*
4. *a glide reflection (that is, a reflection followed by a translation).*

We will come back to this theorem later! (in Chapter 6.)



Main Result (III)

β=H(0)

- $K(0)=\alpha^{-1}(H(0)-\beta)=0$

β=H(0), α=H(1)-H(0)

- $K(1)=\alpha^{-1}(H(1)-\beta)=1$
- K(i) =?

K isometry

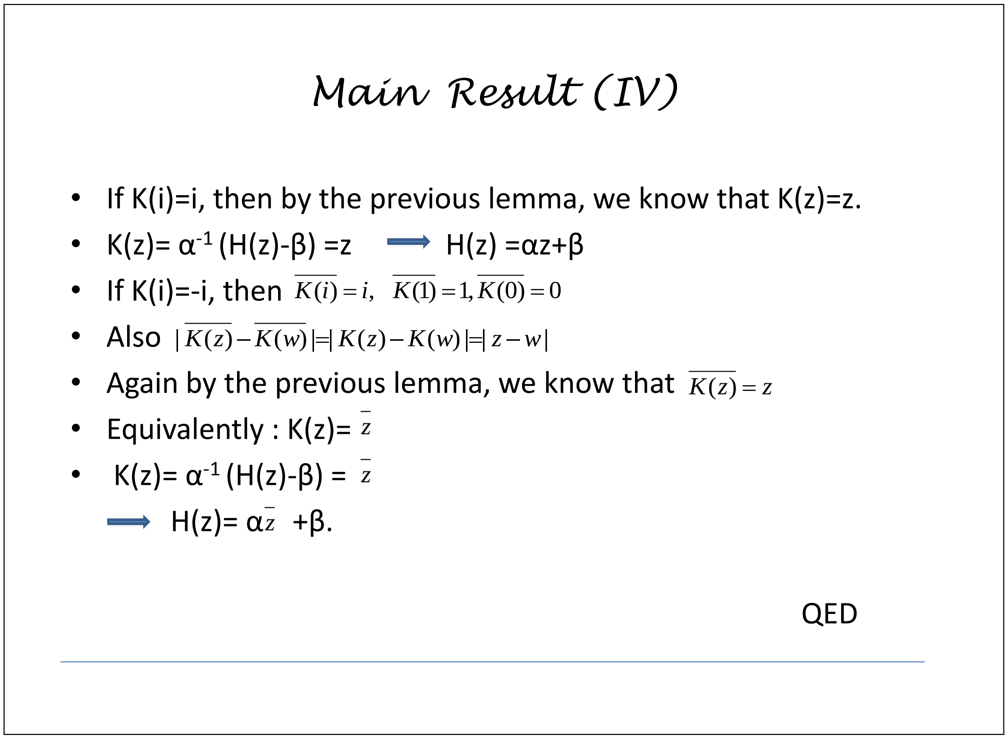
- We know: $|K(i)|=|i|=1$

Why are we computing that? Remember the lemma…

K isometry

- We also know $|K(i)-1|=|i-1|=\sqrt{2}$

$\Rightarrow$ K(i)=i or -i.



Main Result (IV)

- If K(i)=i, then by the previous lemma, we know that K(z)=z.
- $K(z)=\alpha^{-1}(H(z)-\beta)=z \longrightarrow H(z)=\alpha z+\beta$
- If K(i)=-i, then $\overline{K(i)}=i,\ \overline{K(1)}=1, \overline{K(0)}=0$
- Also $|\overline{K(z)}-\overline{K(w)}|=|K(z)-K(w)|=|z-w|$
- Again by the previous lemma, we know that $\overline{K(z)}=z$
- Equivalently : $K(z)=\bar{z}$
- $K(z)=\alpha^{-1}(H(z)-\beta)=\bar{z}$

$\longrightarrow H(z)=\alpha\bar{z}+\beta.$

QED

Next we shall show an easy consequence.

Theorem 3. *Any planar isometry is invertible.*

Proof. We check by direct computation that both possible formulas for isometries, namely

$$H(z) = \alpha z + \beta \text{ and } H(z) = \alpha \overline{z} + \beta, \ \alpha = e^{i\theta}, \beta \in \mathbb{C}$$

are invertible. If $z' = H(z) = \alpha z + \beta$, then

$$z = H^{-1}(z') = \frac{z' - \beta}{\alpha} = e^{-i\theta}(z' - \beta).$$

If instead $z' = H(z) = \alpha \overline{z} + \beta$, then

$$\overline{z} = \frac{z' - \beta}{\alpha} = e^{-i\theta}(z' - \beta)$$

and

$$z = H^{-1}(z') = \overline{e^{-i\theta}}(\overline{z'} - \overline{\beta}).$$

□

Remark. It is important to note that we have shown that a planar isometry is a bijective map. In general, one can define an isometry, but if it is not planar (that is, not from $\mathbb{R}^2$ to $\mathbb{R}^2$), then the definition of isometry usually includes the requirement that the map is bijective by definition. Namely a general isometry is a bijective map which preserves distances.

We now show that we can compose isometries, i.e. apply them one after the other, and that the result of this combination will yield another isometry, i.e., if H_1 and H_2 are two isometries then so is $H_2 H_1$.

Here are two ways of doing so.

First proof. We can use the definition of planar isometry. We want show that $H_2 H_1$ is an isometry. We know that

$$|H_2(H_1(z)) - H_2(H_1(w))| = |H_1(z) - H_1(w)|,$$

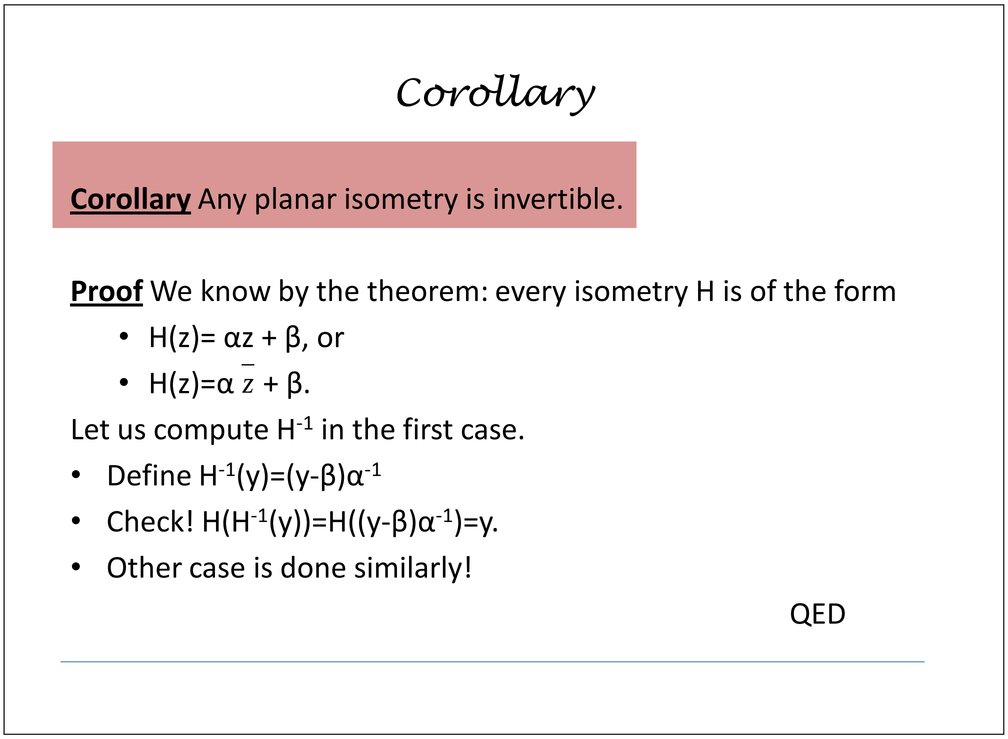
because H_2 is an isometry, and furthermore

$$|H_1(z) - H_1(w)| = |z - w|,$$

this time because H_1 is an isometry. Thus

$$|H_2(H_1(z)) - H_2(H_1(w))| = |z - w|,$$

for any $z, w \in \mathbb{C}$ which completes the proof.



Corollary

Corollary Any planar isometry is invertible.

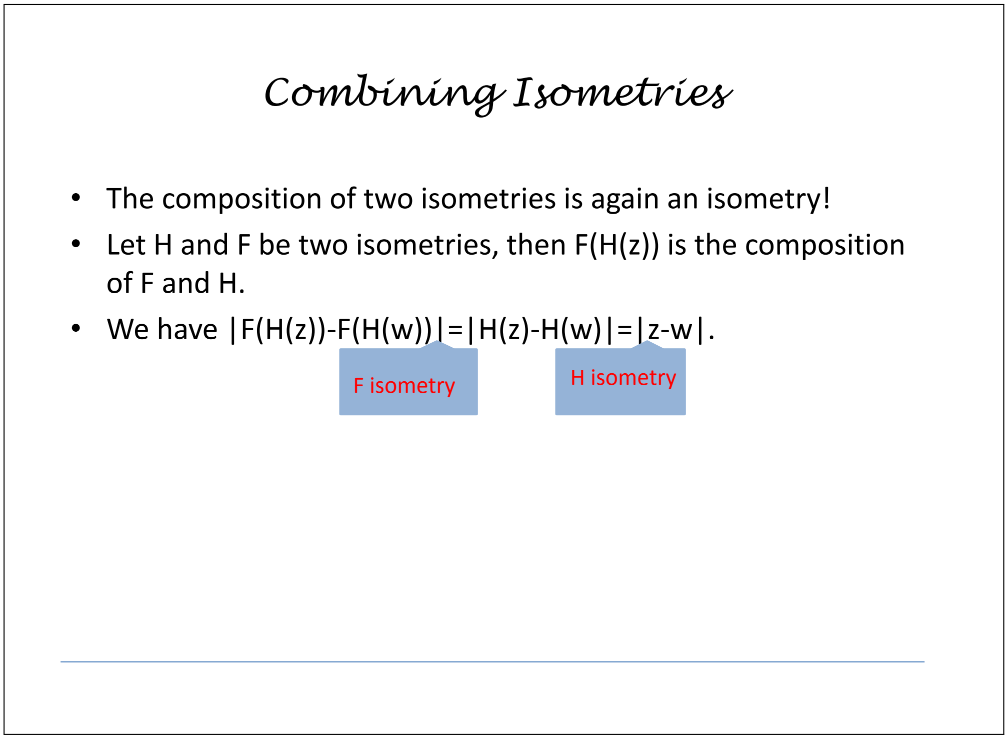
Proof We know by the theorem: every isometry H is of the form

- $H(z)= \alpha z + \beta$, or
- $H(z)=\alpha \bar{z} + \beta$.

Let us compute H^{-1} in the first case.

- Define $H^{-1}(y)=(y-\beta)\alpha^{-1}$
- Check! $H(H^{-1}(y))=H((y-\beta)\alpha^{-1})=y$.
- Other case is done similarly!

QED



Combining Isometries

- The composition of two isometries is again an isometry!
- Let H and F be two isometries, then F(H(z)) is the composition of F and H.
- We have $|F(H(z))-F(H(w))| = |H(z)-H(w)| = |z-w|$.

F isometry
H isometry

Second proof. Alternatively, since H_1, H_2 both have two types (we know that thanks to Theorem 1), there are 4 cases to be verified.

1. $H_2(H_1(z)) = \alpha_2(\alpha_1 z + \beta_1) + \beta_2 = (\alpha_2\alpha_1)z + (\alpha_2\beta_1 + \beta_2)$,
2. $H_2(H_1(z)) = \alpha_2(\alpha_1 \overline{z} + \beta_1) + \beta_2 = (\alpha_2\alpha_1)\overline{z} + (\alpha_2\beta_1 + \beta_2)$,
3. $H_2(H_1(z)) = \alpha_2(\overline{\alpha_1 z} + \overline{\beta_1}) + \beta_2 = (\alpha_2\overline{\alpha_1})\overline{z} + (\alpha_2\overline{\beta_1} + \beta_2)$,
4. $H_2(H_1(z)) = \alpha_2(\overline{\alpha_1} z + \overline{\beta_1}) + \beta_2 = (\alpha_2\overline{\alpha_1})z + (\alpha_2\overline{\beta_1} + \beta_2)$.

In every case, we notice that H_2H_1 is either of the form $\alpha' z+\beta'$, or of the form $\alpha'\overline{z} + \beta'$, which shows that H_1H_2 is an isometry. Indeed, if $H(z) = \alpha' z + \beta'$, then $|H(z)-H(y)| = |\alpha'||z-y| = |z-y|$ (and similarly for $H(z) = \alpha'\overline{z}+\beta'$).

Note that isometries do not commute in general, that is

$$H_2(H_1(z)) \neq H_1(H_2(z))$$

since for example $\alpha_2\beta_1 + \beta_2 \neq \alpha_1\beta_2 + \beta_1$.

But we do have associativity, i.e.

$$H_3(H_2(H_1(z))) = (H_3H_2)(H_1(z)) = H_3(H_2H_1(z)).$$

We also see that the identity map $1 : z \mapsto 1(z) = z$ is an isometry, and when any planar isometry H is composed with its inverse, we obtain as a result the identity map 1:

$$\begin{aligned} H(H^{-1}(z)) &= 1(z) \\ H^{-1}(H(z)) &= 1(z). \end{aligned}$$

What we have proved in fact is that planar isometries form a set of maps which, together with the natural composition of maps, have the following properties:

1. associativity,
2. existence of an identity map (that is a map 1 such that when combined with any other planar isometry H does not change H: $H(1(z)) = 1(H(z)) = z$),
3. inverse for each map.

As we shall see later, this proves that the set of isometries together with the associative binary operation of composition of isometries is a **group**.

Exercises for Chapter 1

Exercise 1. Let X be a metric space equipped with a distance d. Show that an isometry of X (with respect to the distance d) is always an injective map.

Exercise 2. Recall the general formula that describes isometries H of the complex plane. If a planar isometry H has only one fixed point which is $1+i$, and H sends $1-i$ to $3+i$, then $H(z) =$ ________.

Guided version.

1. Recall the general formula that describes isometries H of the complex plane. We saw that an isometry of the complex plane can take two forms, either $H(z) = \ldots$, or $H(z) = \ldots$
2. You should have managed to find the two formulas, because they are in the lecture notes! Now you need to use the assumptions given. First of all, we know that H has only one fixed point, which is $1+i$. Write in formulas what it means that $1+i$ is a fixed point of H (write it for both formulas).
3. Now you must have got one equation from the previous step. Use the next assumption, namely write in formulas what it means that H sends $1-i$ to $3+i$, this should give you a second equation.
4. If all went fine so far, you must be having two equations, with two unknowns, so you are left to solve this system!
5. Once the system is solved, do not forget to check with the original question to make sure your answer is right!

Exercise 3. Recall the general formula that describes isometries H of the complex plane. If a planar isometry H fixes the line $y = x+1$ (identifying the complex plane with the 2-dimensional real plane), then $H(z) =$ ________.

Exercise 4. Show that an isometry of the complex plane that fixes three non-colinear points must be the identity map.

Exercise 5. In this exercise, we study the fixed points of planar isometries. Recall that a planar isometry is of the form $H(z) = \alpha z + \beta$, $H(z) = \alpha \bar{z} + \beta$, $|\alpha| = 1$. Determine the fixed points of these transformations in the different cases that arise:

1. if $H(z) = \alpha z + \beta$ and $\alpha = 1$,
2. if $H(z) = \alpha z + \beta$ and $\alpha \neq 1$
3. if $H(z) = \alpha \bar{z} + \beta$ and $\alpha = 1$, further distinguish $\beta = 0$ and $\beta \neq 0$,
4. if $H(z) = \alpha \bar{z} + \beta$ and $\alpha \neq 1$, further distinguish $\beta = 0$ and $\beta \neq 0$.

Chapter 2

Symmetries of Shapes

"Symmetries delight, please and tease !" (A.M. Bruckstein)

In the previous chapter, we studied planar isometries, that is maps from $\mathbb{R}^2$ to $\mathbb{R}^2$ that are preserving distances. In this chapter, we will focus on different sets of points in the real plane, and see which planar isometries are preserving them.

We are motivated by trying to get a *mathematical formulation* of what is a "nice" regular geometric structure. Intuitively we know of course! We will see throughout this lecture that *symmetries* explain mathematically the geometric properties of figures that we like.

Definition 3. A symmetry of a set of points S in the plane is a planar isometry that preserves S (that is, that maps S to itself).

Note that "symmetries" also appear with letters and numbers! For example, the phrase

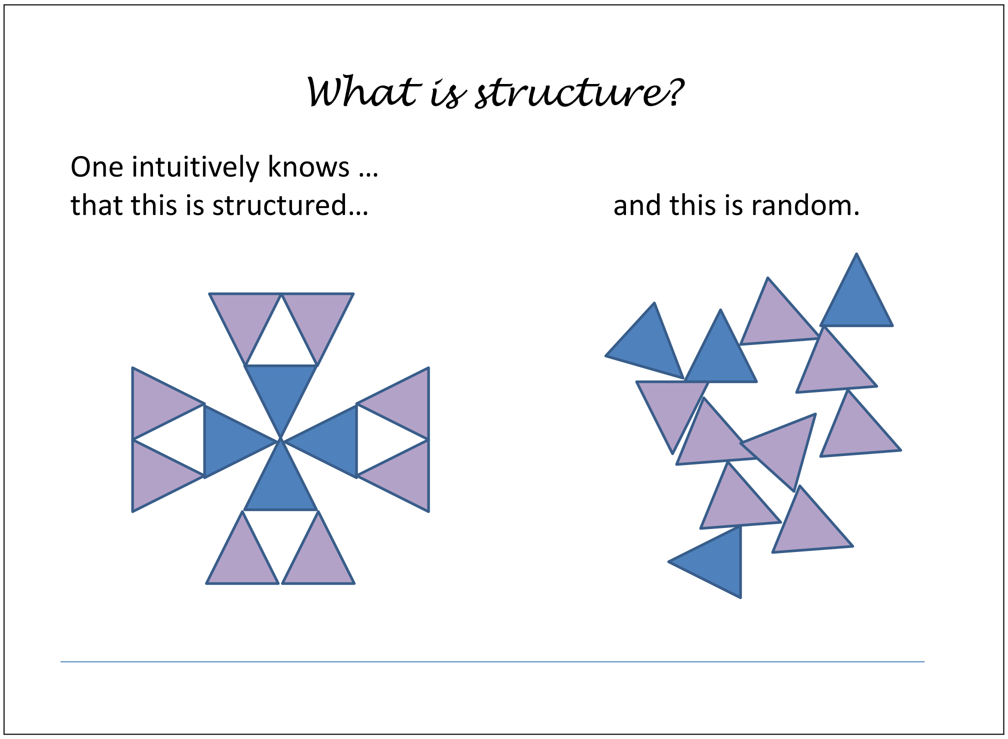
$$NEVER\ ODD\ OR\ EVEN$$

$$\longrightarrow \qquad\qquad \longleftarrow$$

reads the same backwards! It is called a **palindrome**.

The same holds for the number 11311 which happens to be a prime number, called a **palindromic prime**.

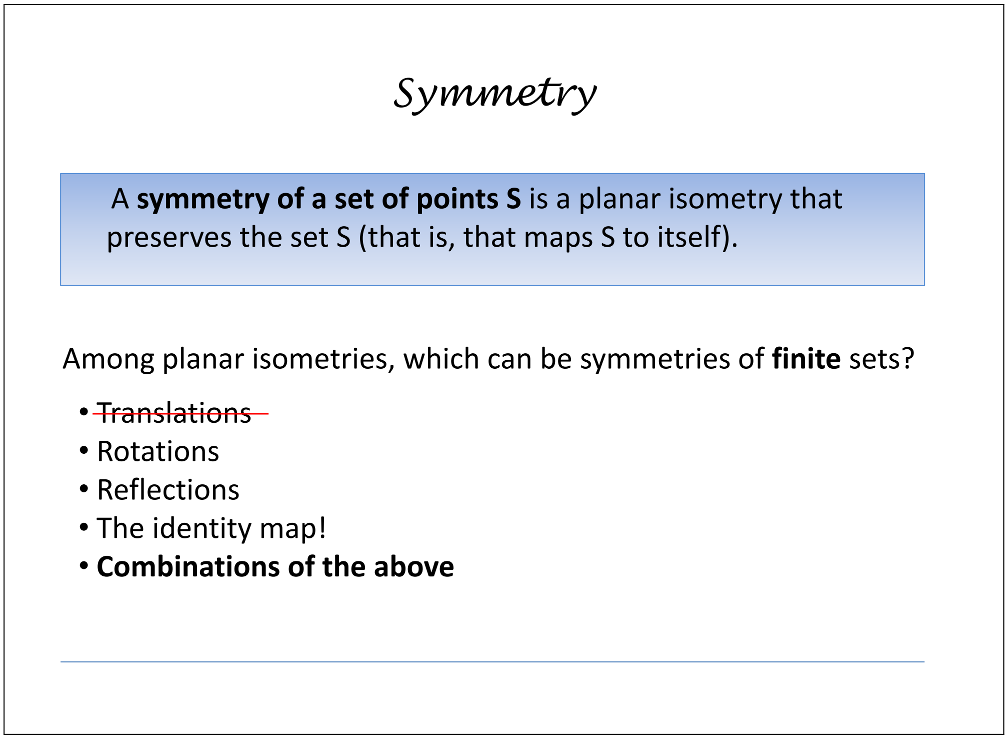
Palindromes can be seen as a conceptual mirror reflection with respect to the vertical axis, which sends a word to itself.



What is structure?

One intuitively knows …
that this is structured…

and this is random.



Symmetry

A **symmetry of a set of points S** is a planar isometry that preserves the set S (that is, that maps S to itself).

Among planar isometries, which can be symmetries of **finite** sets?

- ~~Translations~~
- Rotations
- Reflections
- The identity map!
- **Combinations of the above**

Recall from Theorem 2 that we know all the possible planar isometries, and we know the composition of planar isometries is another planar isometry! All the sets of points that we will consider are finite sets of points centered around the origin, thus we obtain the following list of possible symmetries:

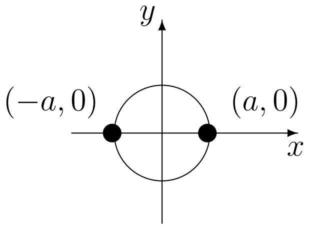
- the trivial identity map $1 : (x, y) \mapsto (x, y)$,
- the mirror reflections $m_v : (x, y) \mapsto (-x, y)$, $m_h : (x, y) \mapsto (-x, y)$ with respect to the y-axis, respectively x-axis, and in fact any reflection around a line passing through the origin,
- the rotation r_ω about 0 counterclockwise by an angle ω

$$\begin{aligned} r_\omega : (x, y) &\mapsto \begin{bmatrix} \cos\omega & -\sin\omega \\ \sin\omega & \cos\omega \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\ &= (x\cos\omega - y\sin\omega, x\sin\omega + y\cos\omega)\,. \end{aligned}$$

Translations are never possible! Consider first the set of points

$$S = \{(a, 0), (-a, 0)\}$$

(shown below) and let us ask what are the symmetries of S.



Clearly the **identity map** is one, it is a planar isometry and $1S = S$. The **mirror reflection** m_v with respect to the y-axis is one as well, since m_v is a planar isometry, and

$$m_v(a, 0) = (-a, 0),\ m_v(-a, 0) = (a, 0) \Rightarrow m_v(S) = S,$$

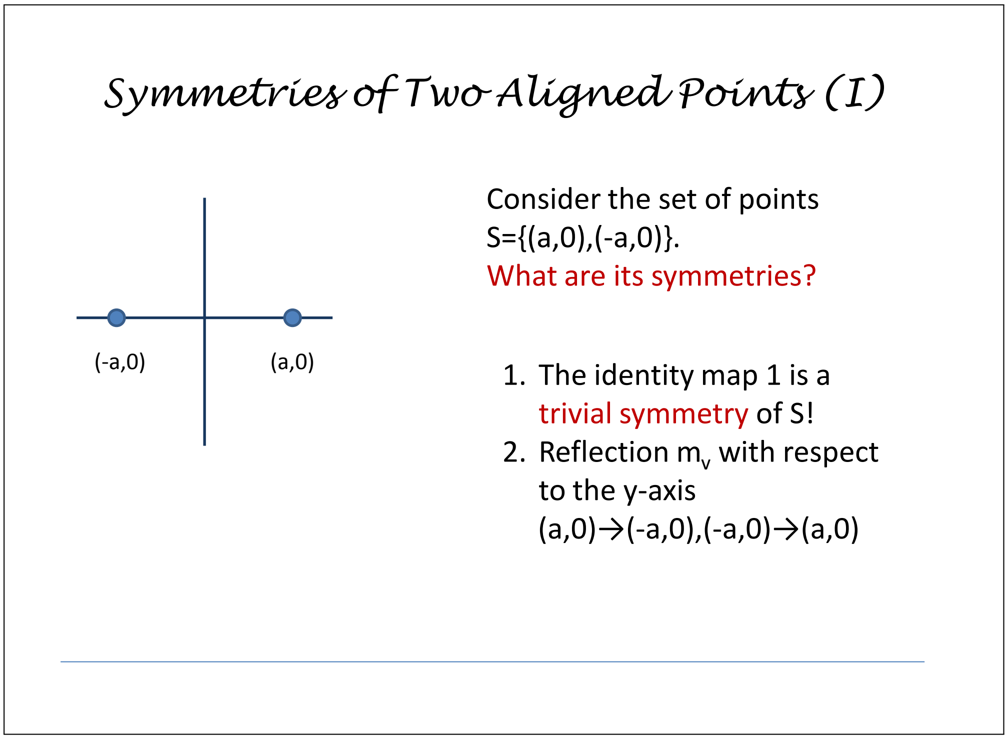
that is S, is **invariant** under m. Now choosing $\omega = \pi$, we have

$$r_\pi(x, y) = (x\cos\pi - y\sin\pi, x\sin\pi + y\cos\pi) = (-x, -y)\,,$$

and

$$r_\pi(a, 0) = (-a, 0),\ r_\pi(-a, 0) = (a, 0) \Rightarrow r_\pi(P) = m_v(P)$$

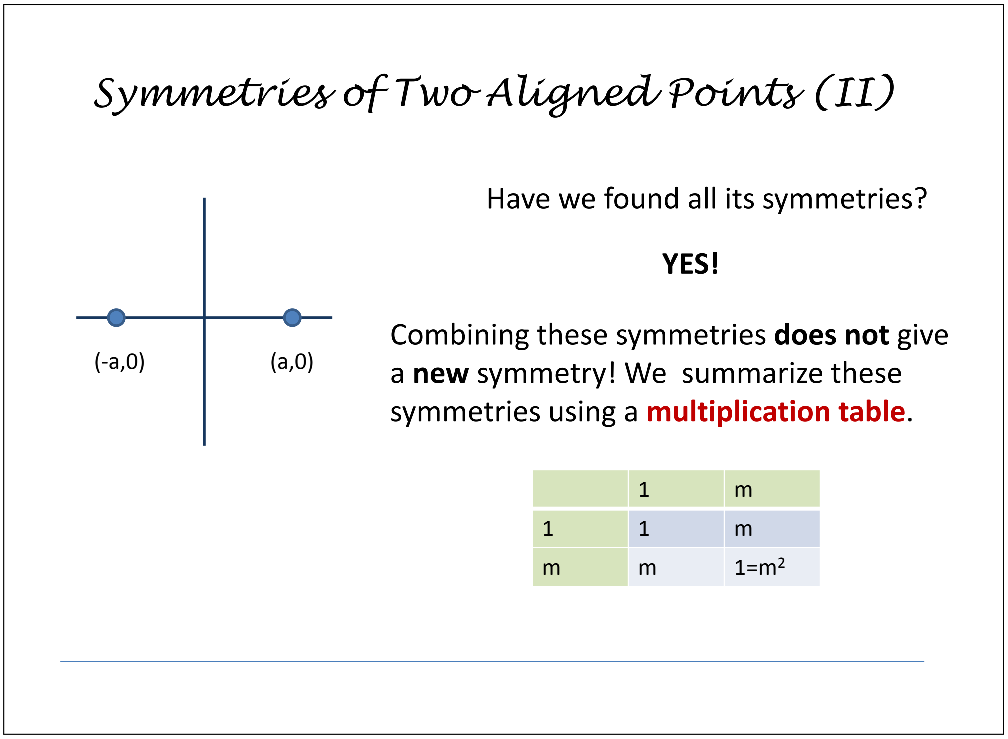
for both points $P \in S$, which shows formally that rotating counterclockwise these two points by π about 0 is the same thing as flipping them around the y-axis.



Symmetries of Two Aligned Points (I)

Consider the set of points S={(a,0),(-a,0)}.
What are its symmetries?

1. The identity map 1 is a trivial symmetry of S!
2. Reflection m_v with respect to the y-axis (a,0)→(-a,0),(-a,0)→(a,0)



Symmetries of Two Aligned Points (II)

Have we found all its symmetries?

YES!

Combining these symmetries **does not** give a **new** symmetry! We summarize these symmetries using a **multiplication table**.

	1	m
1	1	m
m	m	$1=m^2$

We have identified that the set $S = \{(a, 0), (-a, 0)\}$ has 2 symmetries. These are 1 and m_v, or 1 and r_π. We know that planar isometries can be composed, which yields another planar isometry. Then symmetries of S can be composed as well, and here we might wonder what happens if we were to compose m_v with itself:

$$m_v(m_v(x, y)) = m_v(-x, y) = (x, y)$$

which shows that $m_v(m_v(x, y)) = 1(x, y)$. We summarize the symmetries of $S = \{(a, 0), (-a, 0)\}$ using a **multiplication table**:

	1	m_v
1	1	m_v
m_v	m_v	$1 = m_v^2$

The multiplication table is read from left (elements in the column) to right (elements in the row) using as operation the composition of maps.

Let us collect what we have done so far. We defined a set of points $S = \{(a, 0), (-a, 0)\}$ and we looked at three transformations $1, m_v$ and r_π which leave the set of points of $S \in \mathbb{R}^2$ invariant:

$$\begin{cases} 1S = S \\ m_v S = S \\ r_\pi S = S \end{cases} \tag{2.1}$$

We saw that for this particular choice of S, we have that $r_\pi(P) = m_v(P)$ for both points $P \in S$.

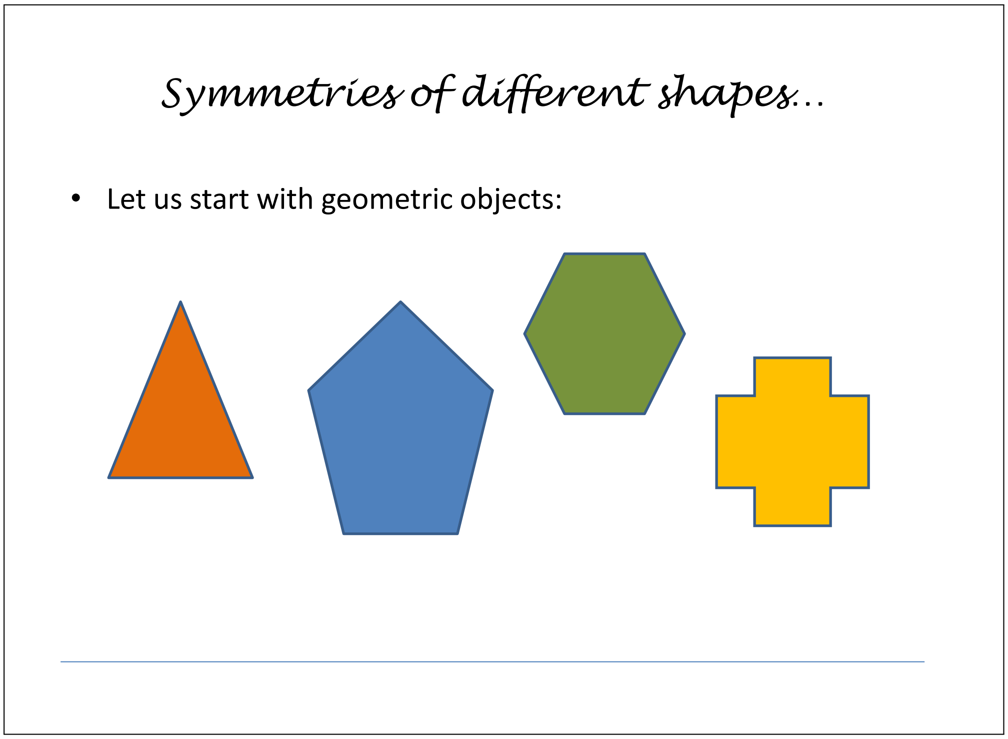
The transformations are however different if we look at a "test point" $(x_0, y_0) \notin S$

$$\begin{cases} 1(x_0, y_0) \to (x_0, y_0) \\ m(x_0, y_0) \to (-x_0, y_0) \\ r_\pi(x_0, y_0) \to (-x_0, -y_0) \end{cases}$$

In fact, one may wonder what happens if we choose for S other sets of points, for example, different polygons. As our next example, we will look at a rectangle S. We write the rectangle S as

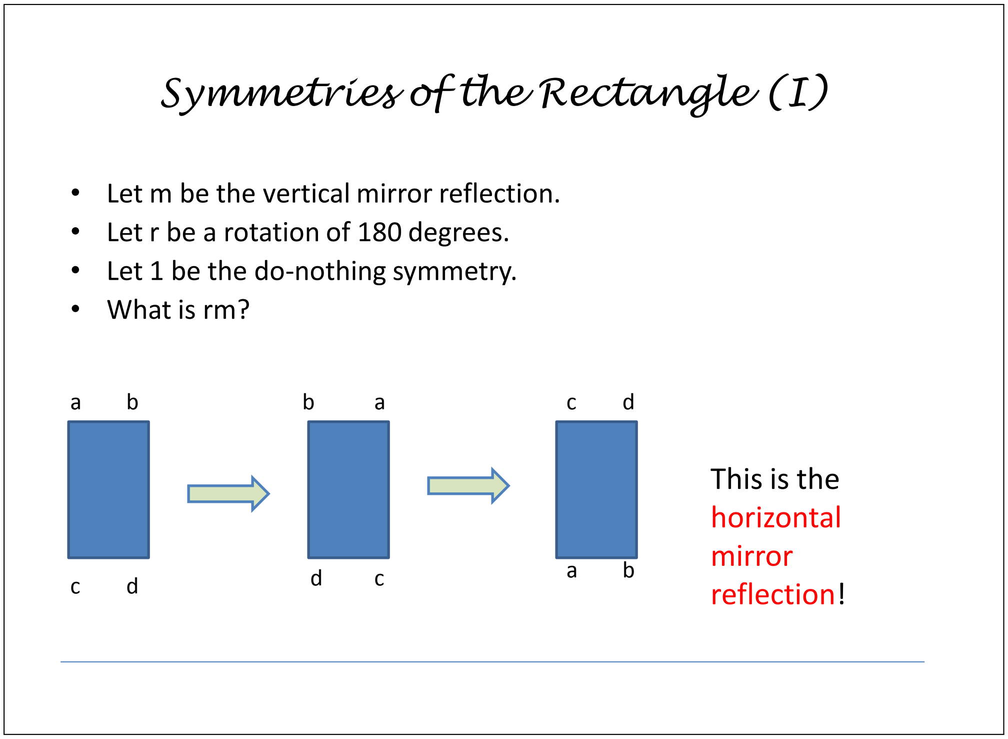
$$S = \{(a, b), (-a, b), (-a, -b), (a, -b)\}\,, \;\; a \neq b, \;\; a, b \neq 0. \tag{2.2}$$

(It is important that $a \neq b$! see (2.3 if $a = b$).)



Symmetries of different shapes…

- Let us start with geometric objects:



Symmetries of the Rectangle (I)

- Let m be the vertical mirror reflection.
- Let r be a rotation of 180 degrees.
- Let 1 be the do-nothing symmetry.
- What is rm?

a b
c d
b a
d c
c d
a b

This is the horizontal mirror reflection!

Let us apply m_v on S:

$$m_v(a,b) = (-a,b),\ m_v(-a,b) = (a,b),$$
$$m_v(-a,-b) = (a,-b),\ m_v(a,-b) = (-a,-b)$$

as well as r_π:

$$r_\pi(a,b) = (-a,-b),\ r_\pi(-a,b) = (a,-b),$$
$$r_\pi(-a,-b) = (a,b),\ r_\pi(a,-b) = (-a,b).$$

These two maps are different and have different effects on S since $r_\pi(a,b) = (-a,-b) \neq (-a,b) = m_v(a,b)$. We now try to compose them. We already have $m_v(m_v(x,y)) = 1(x,y)$, and

$$r_\pi\left(r_\pi(x,y)\right) = r_\pi(-x,-y) = (x,y) = 1(x,y).$$

We continue with

$$r_\pi\left(m_v(x,y)\right) = r_\pi(-x,y) = (x,-y),\ m_v\left(r_\pi(x,y)\right) = m_v(-x,-y) = (x,-y)$$

which both give **a horizontal mirror reflection** m_h, also showing that

$$r_\pi m_v = m_v r_\pi = m_h,$$

i.e., the transformations r_π and m_v commute. In turn, we immediately have

$$(r_\pi m_v)^2 = r_\pi m_v r_\pi m_v = r_\pi m_v m_v r_\pi = r_\pi 1 r_\pi = r_\pi r_\pi = 1.$$

The rules for combining elements from $\{1, m_v, r_\pi, m_v r_\pi\}$

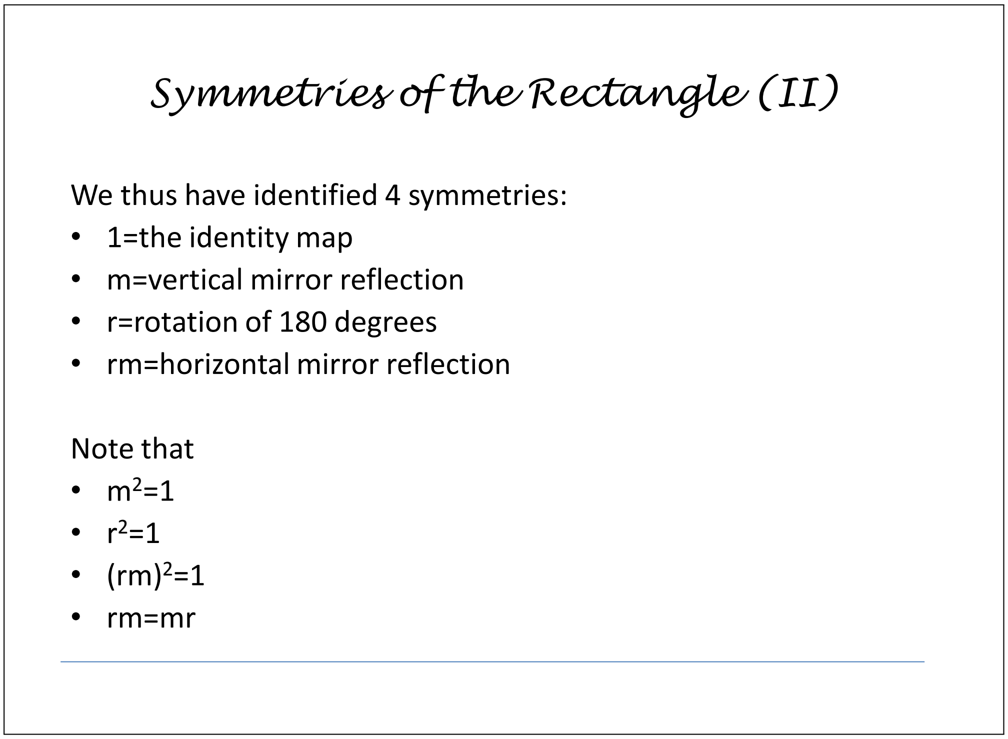
$$\begin{cases} m_v 1 = m_v = 1 m_v \\ r_\pi 1 = r_\pi = 1 r_\pi \\ m_v^2 = 1 \\ r_\pi^2 = 1 \\ m_v r_\pi = r_\pi m_v \end{cases}$$

show that no new transformations will ever be obtained since we have

$$r_\pi^{(\alpha_i)} = r_\pi^{\alpha_i \mod 2},\ m_v^{(\beta_i)} = m_v^{\beta_i \mod 2},\ \pi^{\alpha_1} m_v^{\beta_1} r_\pi^{\alpha_2} m_v^{\beta_2} \cdots = r_\pi^{(\sum \alpha_i) \mod 2} m_v^{(\sum \beta_i) \mod 2}.$$

Hence we have obtained a complete set of transformations for the shape S summarized in its multiplication table (we write $m = m_v$ for short):

	1	m	r_π	mr_π
1	1	m	r_π	mr_π
m	m	1	mr_π	r_π
r_π	r_π	mr_π	1	m
mr_π	mr_π	r_π	m	1



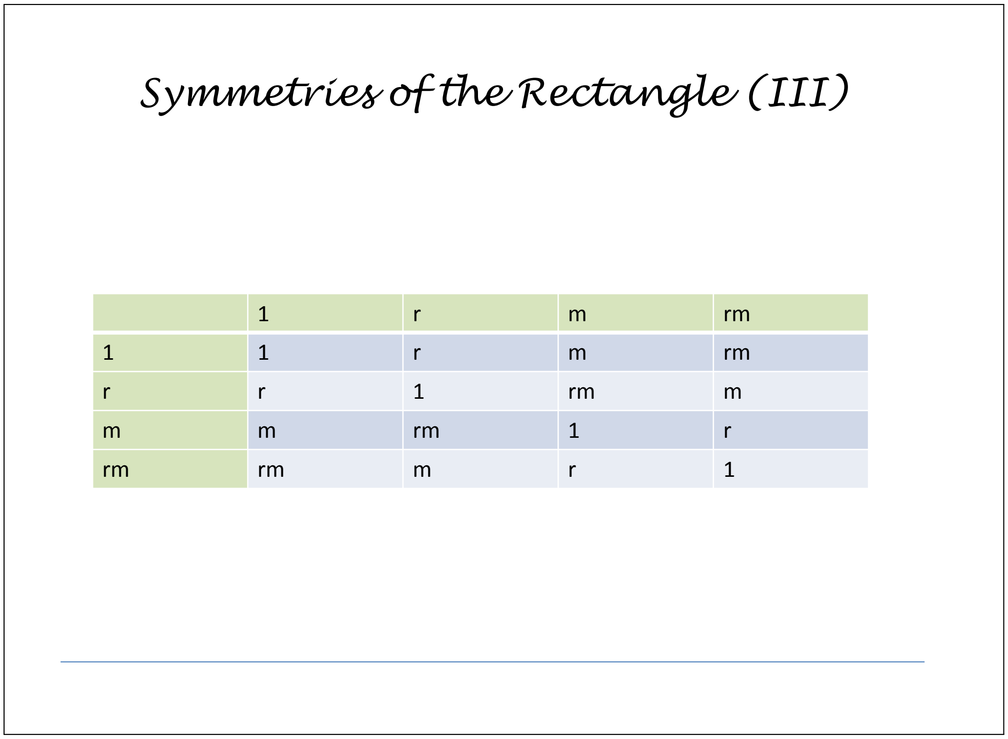
Symmetries of the Rectangle (II)

We thus have identified 4 symmetries:

- 1=the identity map
- m=vertical mirror reflection
- r=rotation of 180 degrees
- rm=horizontal mirror reflection

Note that

- m^2=1
- r^2=1
- $(rm)^2$=1
- rm=mr



Symmetries of the Rectangle (III)

	1	r	m	rm
1	1	r	m	rm
r	r	1	rm	m
m	m	rm	1	r
rm	rm	m	r	1

We next study the symmetries of a square, that is we consider the set

$$S_4 : \{(a,a),(-a,a),(a,-a)(-a,-a)\} \tag{2.3}$$

(this is the case where $a=b$ in (2.2)).

As for the two previous examples, we first need to see what are all the planar isometries we need to consider. There are four mirror reflections that map S_4 to itself:

$$\begin{array}{rcl} m_1 = m_v : & (x,y) \mapsto (-x,y) & \text{with respect to the } y\text{-axis} \\ m_2 : & (x,y) \mapsto (y,x) & \text{with respect to the line } y=x \\ m_3 = m_h : & (x,y) \mapsto (x,-y) & \text{with respect to the } x\text{-axis} \\ m_4 : & (x,y) \mapsto (-y,-x) & \text{with respect to the line } y=-x \end{array}$$

Note that

$$m_i(m_i(x,y)) = 1(x,y),\ i=1,2,3,4.$$

There are also three (counterclockwise) rotations (about the origin 0=(0,0)):

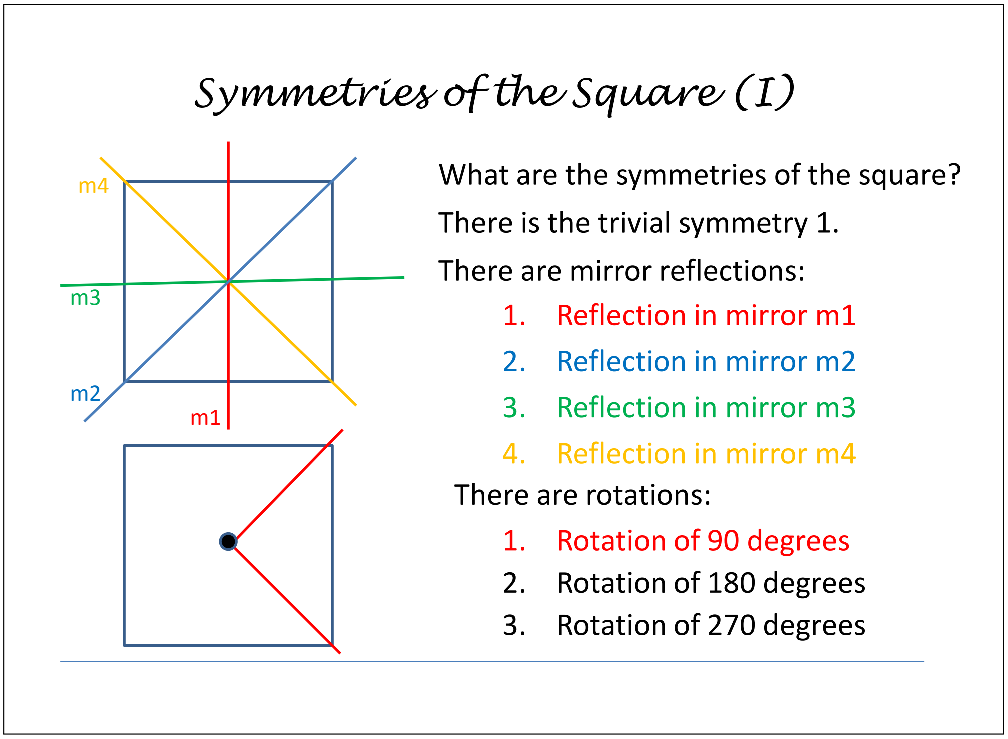
$$\begin{array}{rc} r_{\pi/2} : & (x,y) \mapsto (x\cos\pi/2 - y\sin\pi/2, x\sin\pi/2 + y\cos\pi/2) = (-y,x) \\ r_{\pi} : & (x,y) \mapsto (x\cos\pi - y\sin\pi, x\sin\pi + y\cos\pi) = (-x,-y) \\ r_{3\pi/2} : & (x,y) \mapsto (x\cos 3\pi/2 - y\sin 3\pi/2, x\sin 3\pi/2 + y\cos 3\pi/2) = (y,-x) \end{array}$$

and $r_{2\pi}=1$. Rotations are easy to combine among each others! For example

$$\begin{array}{rcl} r_{\pi} & = & r_{\pi/2}r_{\pi/2} \\ r_{3\pi/2} & = & r_{\pi/2}r_{\pi/2}r_{\pi/2} \end{array}$$

and we can give the part of the multiplication table which involves only rotations. We summarize all the rotations by picking one rotation r whose powers contain the 4 rotations $r_{\pi/2}, r_{\pi}, r_{3\pi/2}, 1$. We can choose $r = r_{\pi/2}$ and $r = r_{3\pi/2}$, though in what follows we will focus on $r = r_{3\pi/2} = r_{-\pi/2}$, the rotation of 90 degrees clockwise, or 270 degrees counterclockwise:

	1	r	r^2	r^3
1	1	r	r^2	r^3
r	r	r^2	r^3	1
r^2	r^2	r^3	1	r
r^3	r^3	1	r	r^2



Symmetries of the Square (I)

What are the symmetries of the square?

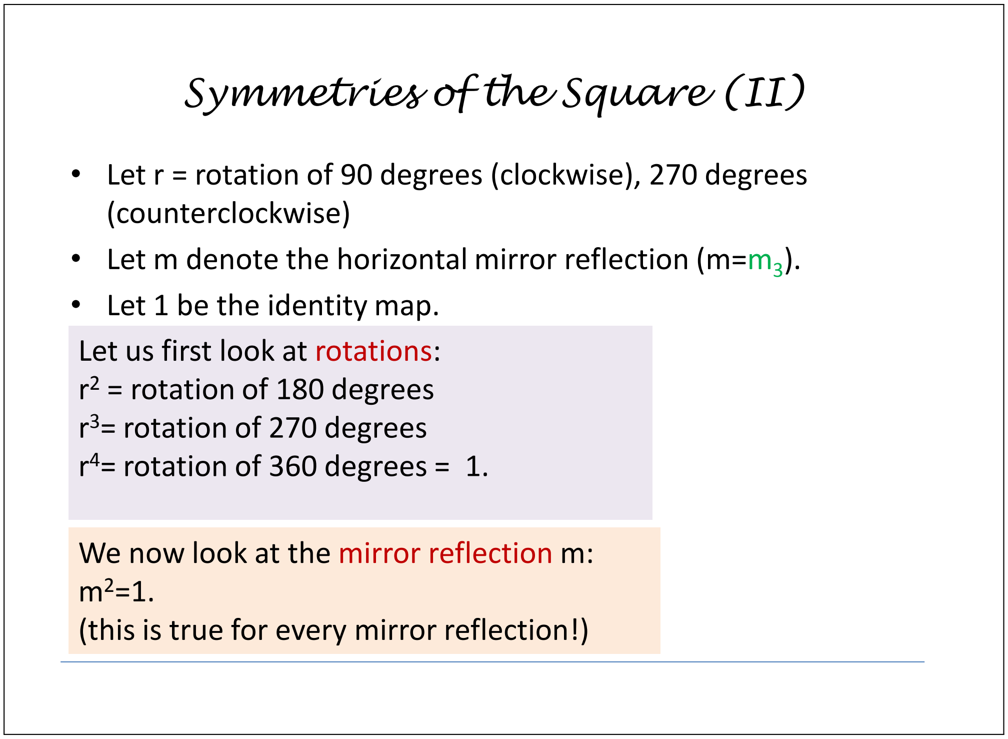
There is the trivial symmetry 1.

There are mirror reflections:

1. Reflection in mirror m1
2. Reflection in mirror m2
3. Reflection in mirror m3
4. Reflection in mirror m4

There are rotations:

1. Rotation of 90 degrees
2. Rotation of 180 degrees
3. Rotation of 270 degrees



Symmetries of the Square (II)

- Let r = rotation of 90 degrees (clockwise), 270 degrees (counterclockwise)
- Let m denote the horizontal mirror reflection ($m=m_3$).
- Let 1 be the identity map.

Let us first look at rotations:
r^2 = rotation of 180 degrees
r^3= rotation of 270 degrees
r^4= rotation of 360 degrees = 1.

We now look at the mirror reflection m:
$m^2=1$.
(this is true for every mirror reflection!)

Let us try to compose mirror reflections with rotations. For that, we pick first

$$m = m_h : (x, y) \mapsto (x, -y),\ r = r_{3\pi/2} : (x, y) \mapsto (y, -x),$$

and compute what is rm and mr (you can choose to do the computations with another reflection instead of m_h, or with $r = r_{\pi/2}$ instead of $r = r_{3\pi/2}$.) We get

$$r(m(x, y)) = r(x, -y) = (-y, -x),\ m(r(x, y)) = m(y, -x) = (y, x)$$

and since $S_4 = \{(a, a), (-a, a), (a, -a)(-a, -a)\}$, we see that for example

$$r(m(a, a)) = (-a, -a),\ m(r(a, a)) = (a, a)$$

and these two transformations are different! We also notice something else which is interesting:

$$rm = m_4 = \text{reflection with respect to the line } y = -x$$

and

$$mr = m_2 = \text{reflection with respect to the line } y = x.$$

Since $rm \neq mr$ and we want to classify all the symmetries of the square S_4, we need to fix an ordering to write the symmetries in a systematic manner. We choose to first write a mirror reflection, and second a rotation (you could choose to first write a rotation and second a mirror reflection, what matters is that both ways allow you to describe all the symmetries, as we will see now!) This implies that we will look at all the possible following symmetries, written in the chosen ordering:

$$rm,\ r^2m,\ r^3m.$$

We have just computed rm, so next we have

$$r^2m(x, y) = r^2(x, -y) = r(-y, -x) = (-x, y) \tag{2.4}$$

and by applying r once more on (2.4) we get

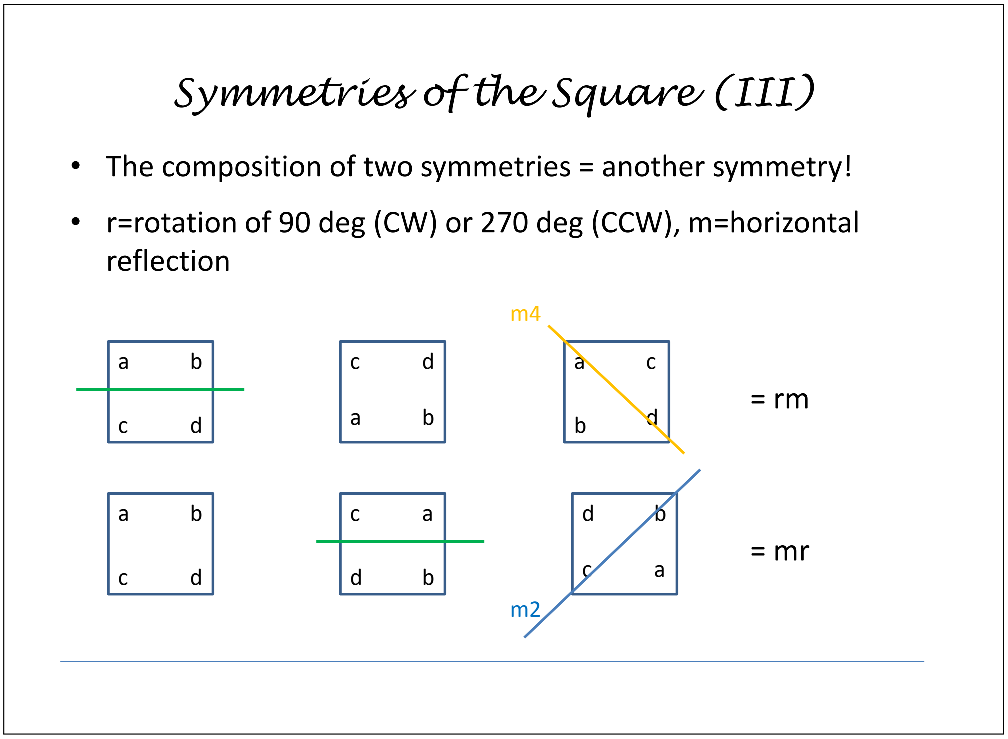
$$r^3m(x, y) = r(-x, y) = (y, x)$$

showing that

$$r^2m = \text{reflection with respect to the } y{-}axis$$

and

$$r^3m = mr = \text{reflection with respect to the line } y = x.$$

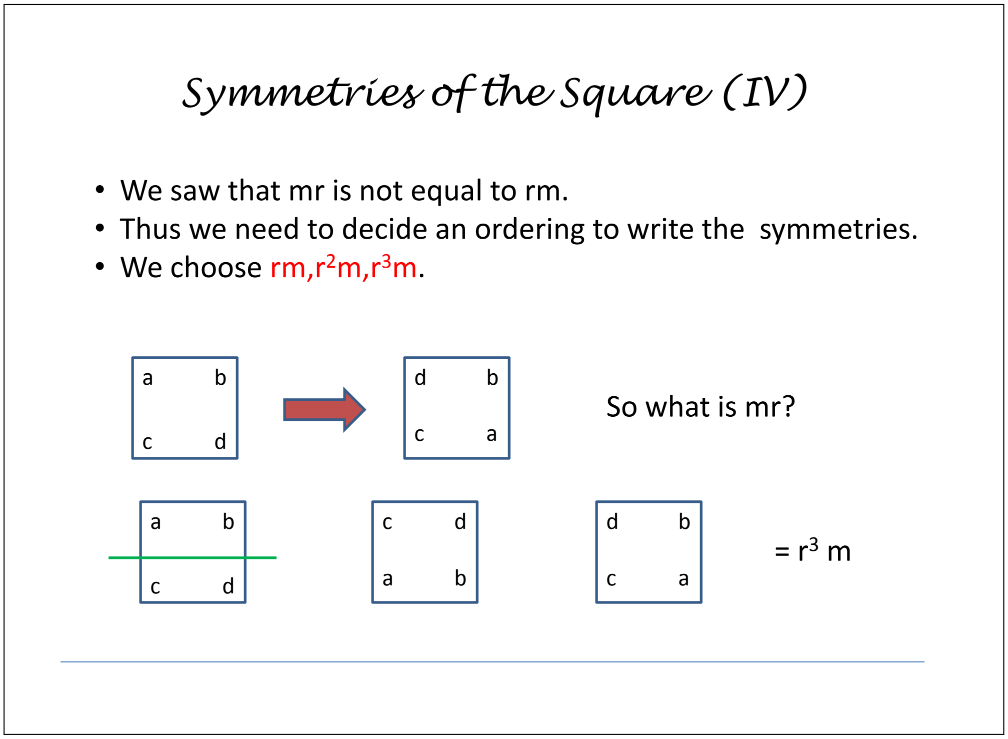


Symmetries of the Square (III)

- The composition of two symmetries = another symmetry!
- r=rotation of 90 deg (CW) or 270 deg (CCW), m=horizontal reflection

= rm

= mr



Symmetries of the Square (IV)

- We saw that mr is not equal to rm.
- Thus we need to decide an ordering to write the symmetries.
- We choose rm, r^2m, r^3m.

So what is mr?

= r^3 m

It is a good time to start summarizing all what we have been doing!

Step 1. We recognize that among all the planar isometries, there are 8 of them that are symmetries of the square S_4, namely:

1. m_1= reflection with respect to the y-axis,
2. m_2= reflection with respect to the line $y = x$,
3. m_3= reflection with respect to the x-axis,
4. m_4= reflection with respect to the line $y = -x$,
5. the rotation $r_{\pi/2}$,
6. the rotation r_π,
7. the rotation $r_{3\pi/2}$,
8. and of course the identity map 1!

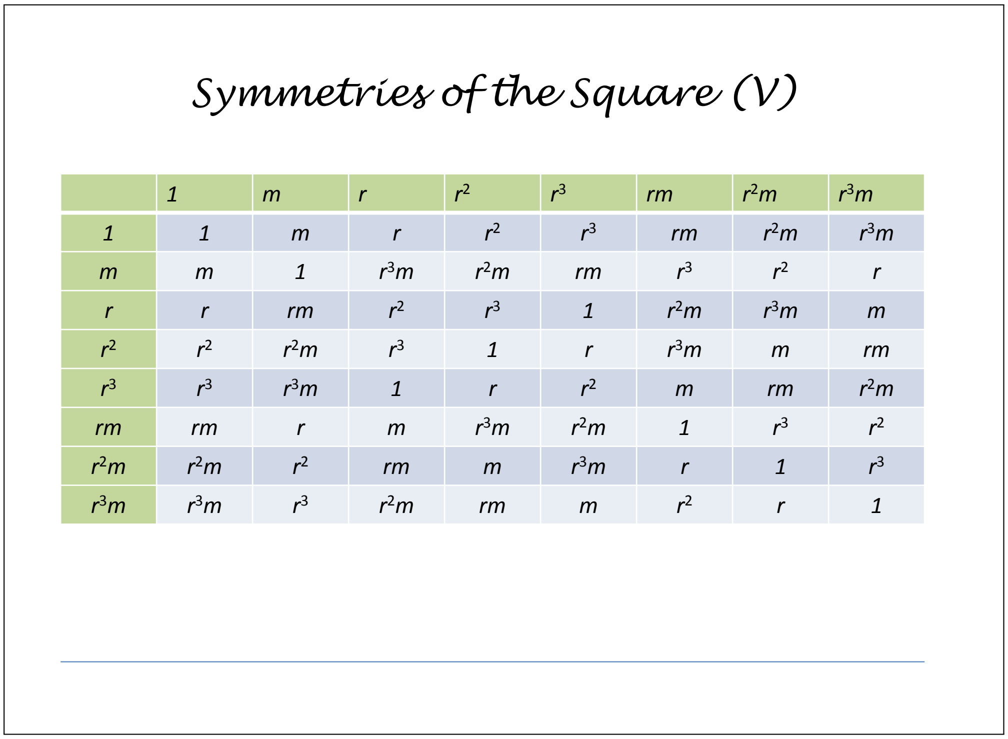
Step 2. We fixed $m = m_3$ and $r = r_{3\pi/2}$ and computed all the combinations of the form $r^i m^j$, $i = 1, 2, 3, 4$, $j = 1, 2$, and we found that

$$\begin{aligned} rm &= m_4 \\ r^2m &= m_1 \\ r^3m &= m_2 \end{aligned}$$

which means that we can express all the above 8 symmetries of the square as $r^i m^j$, and furthermore, combining them does not give new symmetries!

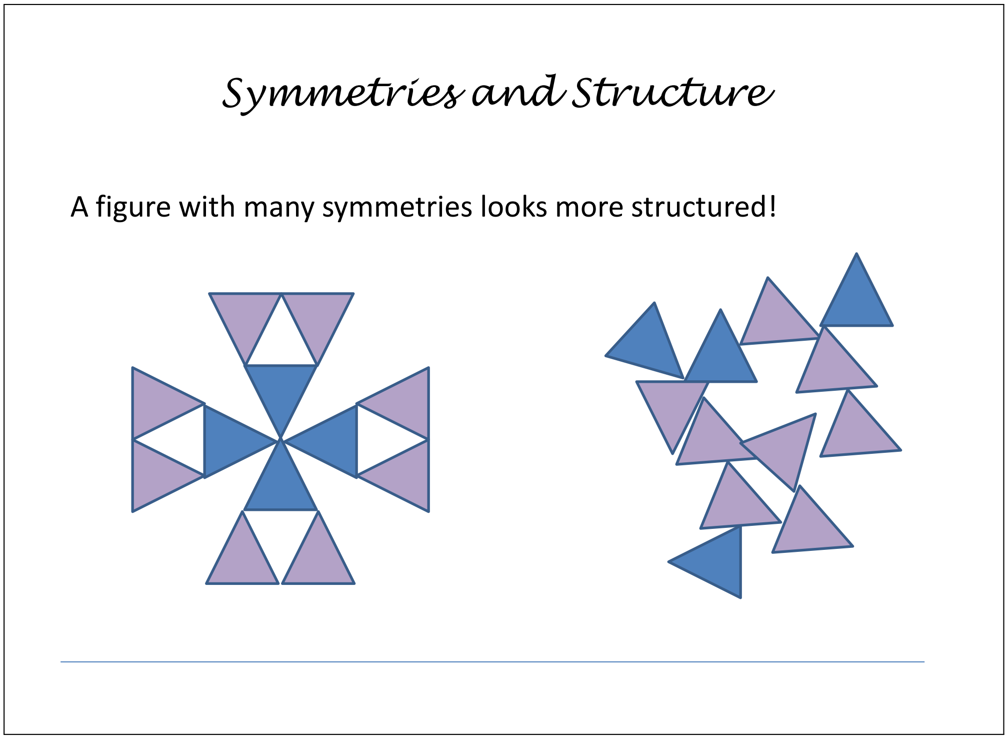
We can thus summarize all the computations in the following multiplication table.

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1



Symmetries of the Square (V)

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1



Symmetries and Structure

A figure with many symmetries looks more structured!

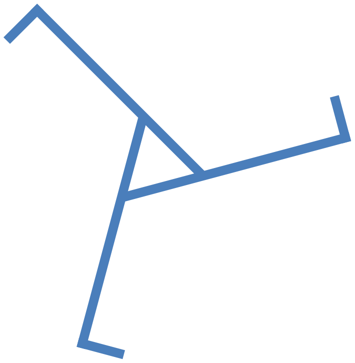
In the first chapter, we defined and classified planar isometries. Once we know what are all the possible isometries of plane, in this chapter, we focus on a subset of them: given a set of points S, what is the subset of planar isometries that preserves S. We computed three examples: (1) the symmetries of two points, (2) the symmetries of the rectangle, and (3) that of the square. We observed that the square has more symmetries (8 of them!) than the rectangle (4 of them). In fact, the more "regular" the set of points is, the more symmetries it has, and somehow, the "nicer" this set of points look to us!

Exercises for Chapter 2

Exercise 6. Determine the symmetries of an isosceles triangle, and compute the multiplication table of all its symmetries.

Exercise 7. Determine the symmetries of an equilateral triangle, and compute the multiplication table of all its symmetries.

Exercise 8. Determine the symmetries of the following shape, and compute the multiplication table of all its symmetries.



Exercise 9. Let $z = e^{2i\pi/3}$.

1. Show that $z^3 = 1$.
2. Compute the multiplication table of the set $\{1, z, z^2\}$.
3. Compare your multiplication table with that of Exercise 8. What can you observe? How would you interpret what you can see?

Exercise 10. In the notes, we computed the multiplication table for the symmetries of the square. We used as convention that entries in the table are of the form $r^i m^j$. Adopt the reverse convention, that is, write all entries as $m^j r^i$ and recompute the multiplication table. This is a good exercise if you are not yet comfortable with these multiplication tables!

Chapter 3

Introducing Groups

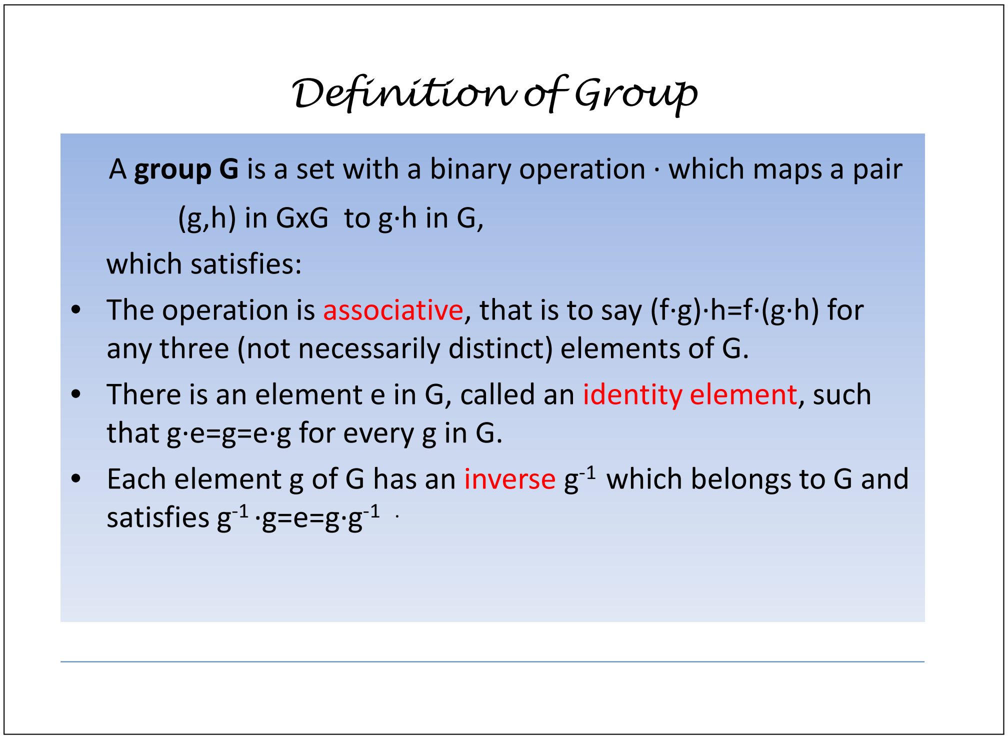
> *"We need a super-mathematics in which the operations are as unknown as the quantities they operate on, and a super-mathematician who does not know what he is doing when he performs these operations. Such a super-mathematics is the Theory of Groups." (Sir Arthur Stanley Eddington, physicist)*

The first two chapters dealt with planar geometry. We identified what are the possible planar isometries, and then, given a set S of points in the plane, we focused on the subset of planar isometries that preserves this given set S. These are called symmetries of S. We saw that planar isometries, respectively symmetries, can be composed to yield another planar isometry, respectively symmetry. Every planar isometry is invertible. Every symmetry of a given set S is invertible as well, with as inverse another symmetry of S.

We now put a first step into the world of abstract algebra, and introduce the notion of a *group*. We will see soon that groups have close connections with symmetries!

Definition 4. A group G is a set with a binary operation (law) $\cdot$ satisfying the following conditions:

1. For all $g_1, g_2 \in G \Rightarrow g_1 \cdot g_2 \in G$.
2. The binary law is associative.
3. There is an *identity* element e in G, such that $g \cdot e = e \cdot g = g$, $\forall g \in G$.
4. Every element $g \in G$ has an *inverse* g^{-1}, such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

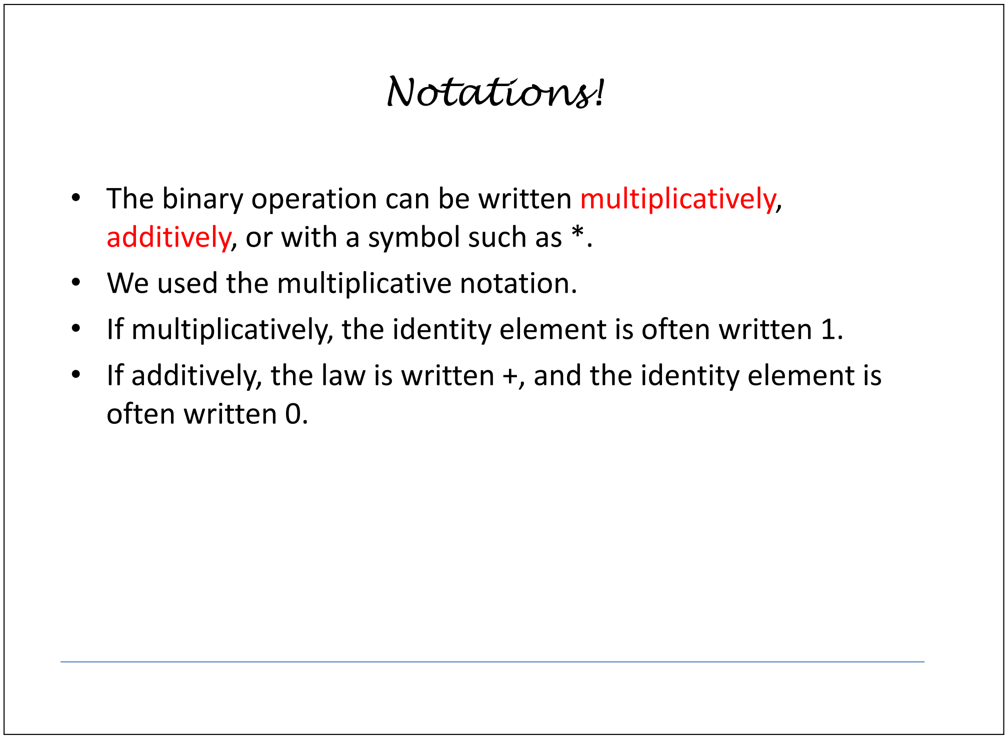


Definition of Group

A **group G** is a set with a binary operation $\cdot$ which maps a pair (g,h) in $G\times G$ to $g\cdot h$ in G,

which satisfies:

- The operation is associative, that is to say $(f\cdot g)\cdot h=f\cdot(g\cdot h)$ for any three (not necessarily distinct) elements of G.
- There is an element e in G, called an identity element, such that $g\cdot e=g=e\cdot g$ for every g in G.
- Each element g of G has an inverse g^{-1} which belongs to G and satisfies $g^{-1}\cdot g=e=g\cdot g^{-1}$.



Notations!

- The binary operation can be written multiplicatively, additively, or with a symbol such as *.
- We used the multiplicative notation.
- If multiplicatively, the identity element is often written 1.
- If additively, the law is written +, and the identity element is often written 0.

There are many things to comment about this definition! We understand what a set G means. Now we consider this set together with a binary operation (also called binary law). This binary operation can be different things, depending on the nature of the set G. As a result, this operation can be denoted in different ways as well. Let us see some of them. We will write the set and the law as a pair, to make explicit the binary operation:

- In multiplicative notation, we write $(G, \cdot)$, and the identity element is often written 1, or 1_G if several groups and their identity elements are involved.
- In additive notation, we write $(G, +)$, and the identity element is often written 0, or 0_G.
- There could be more general notations, such as $(G, *)$, when we want to emphasize that the operation can be very general.

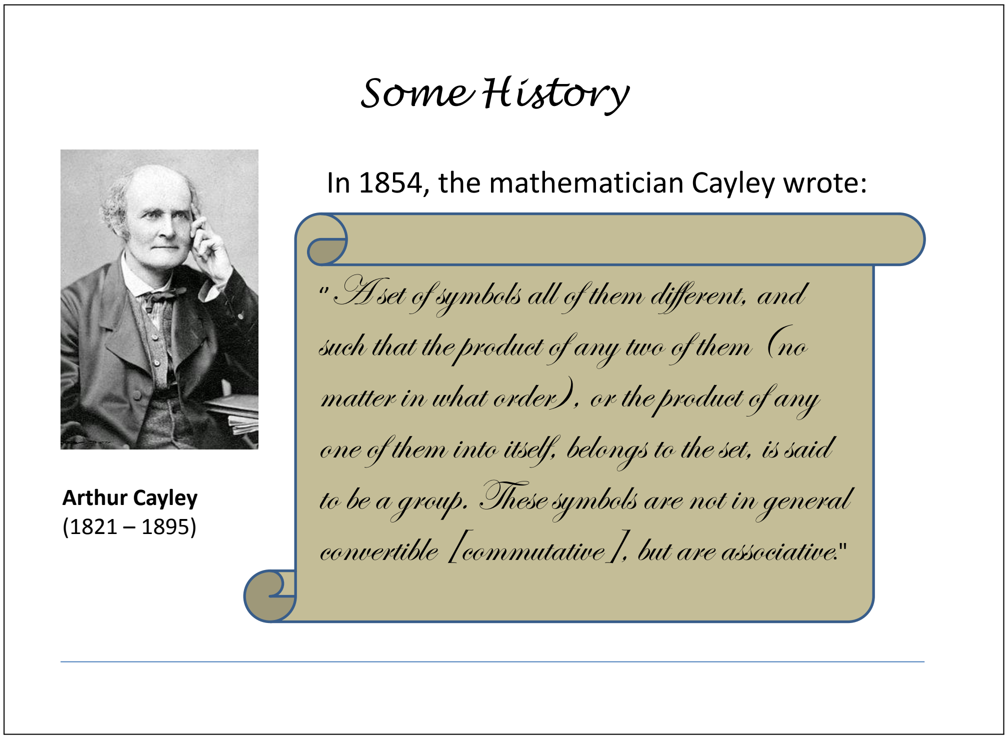
The multiplicative notation *really is* a notation! For example, if m denotes a mirror rotation and r a rotation, the notation $r \cdot m$ (or in fact rm for short) means *the composition of maps*, since multiplying these maps does not make sense! It is thus important to understand the meaning of the formalism that we are using!

There are 4 key properties in the definition of group. Let us use the multiplicative notation here, that is we have a group $(G, \cdot)$.

1. If we take two elements in our group G, let us call them g_1, g_2, then $g_1 \cdot g_2$ must belong to G.
2. The binary operation that we consider must be associative.
3. There must exist an identity element.
4. Every element must have an inverse.

If any of these is not true, then we do not have a group structure.

It is interesting to notice that the modern definition of group that we just saw was in fact proposed by the mathematician Cayley, back in 1854!

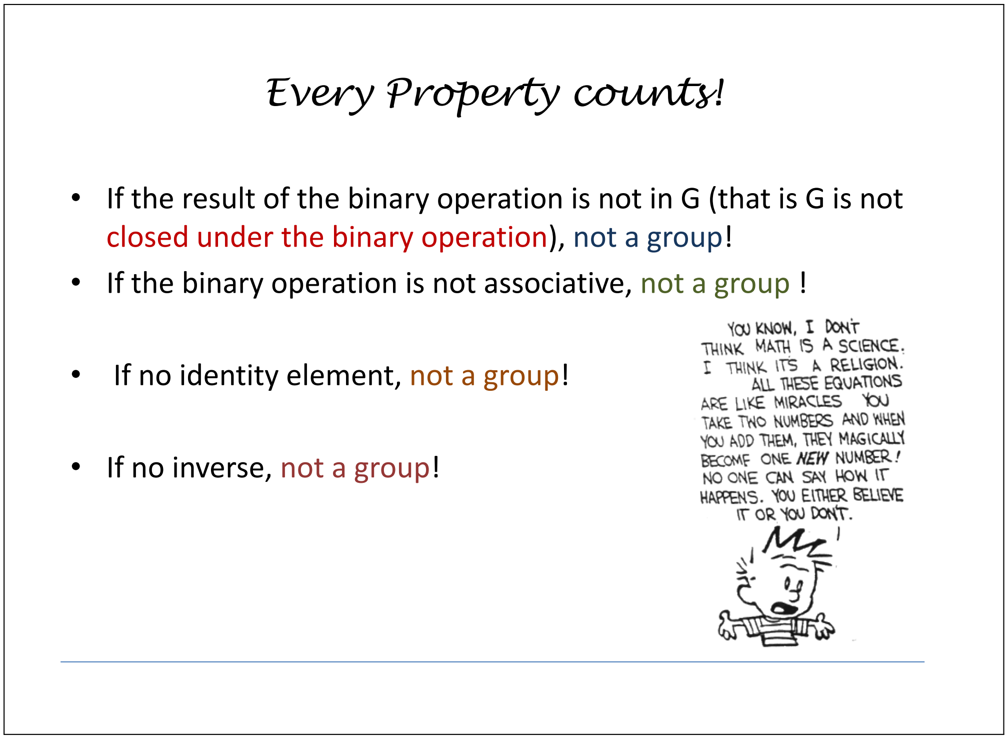


Some History

In 1854, the mathematician Cayley wrote:

> "*A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative.*"

Arthur Cayley
(1821 – 1895)



Every Property counts!

- If the result of the binary operation is not in G (that is G is not closed under the binary operation), not a group!
- If the binary operation is not associative, not a group !
- If no identity element, not a group!
- If no inverse, not a group!

YOU KNOW, I DON'T THINK MATH IS A SCIENCE. I THINK IT'S A RELIGION. ALL THESE EQUATIONS ARE LIKE MIRACLES. YOU TAKE TWO NUMBERS AND WHEN YOU ADD THEM, THEY MAGICALLY BECOME ONE *NEW* NUMBER! NO ONE CAN SAY HOW IT HAPPENS. YOU EITHER BELIEVE IT OR YOU DON'T.

To get used to the formalism of the group definition, let us try to make a small proof.

Proposition 1. *Let* $(G, \cdot)$ *be a group, with identity element* e. *Then this identity element is unique.*

Proof. To prove that e is unique, we will assume that there is another identity element e', and show that $e = e'$. Let us thus do so, and assume that both e and e' are identity elements of G.

We now recall what is the definition of an identity element. If e is an identity element, then it must satisfy

$$e \cdot g = g \cdot e = g \tag{3.1}$$

for every element g of G, and e' must similarly satisfy

$$e' \cdot g = g \cdot e' = g \tag{3.2}$$

for every element g of G.

Now we know that (3.1) is true for every element in G, thus it is true for e' as well, and

$$e \cdot e' = e'.$$

We redo the same thing with e'. Because (3.2) is true for every element in G, then it is true for e, which gives

$$e \cdot e' = e.$$

Now we put these two equations together, to obtain

$$e \cdot e' = e' = e \Rightarrow e' = e.$$

□

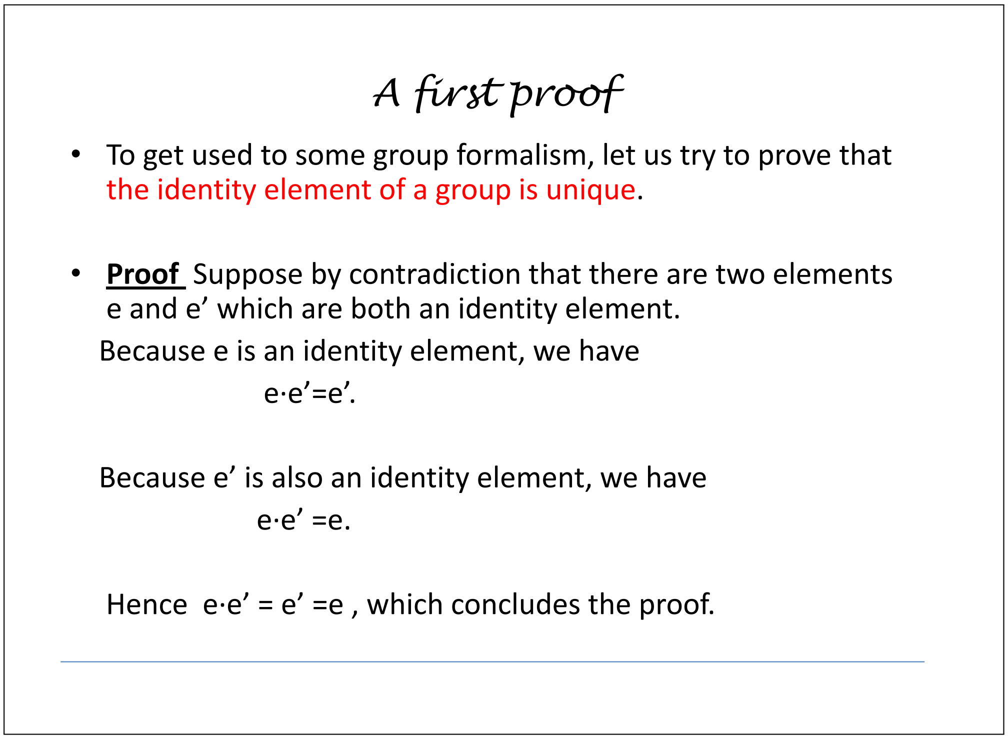
A group becomes much simpler to understand if its binary operation is in fact commutative. We give such groups a particular name.

Definition 5. Let $(G, \cdot)$ be a group. If the binary operation $\cdot$ is commutative, i.e., if we have

$$\forall g_1, g_2 \in G, \quad g_1 \cdot g_2 = g_2 \cdot g_1,$$

then the group is called **commutative** or **abelian** (in honor of the mathematician Abel (1802-1829)).

When a group is abelian, its binary operation is often denoted additively, that is $(G, +)$.



A first proof

- To get used to some group formalism, let us try to prove that the identity element of a group is unique.

- **Proof** Suppose by contradiction that there are two elements e and e’ which are both an identity element.

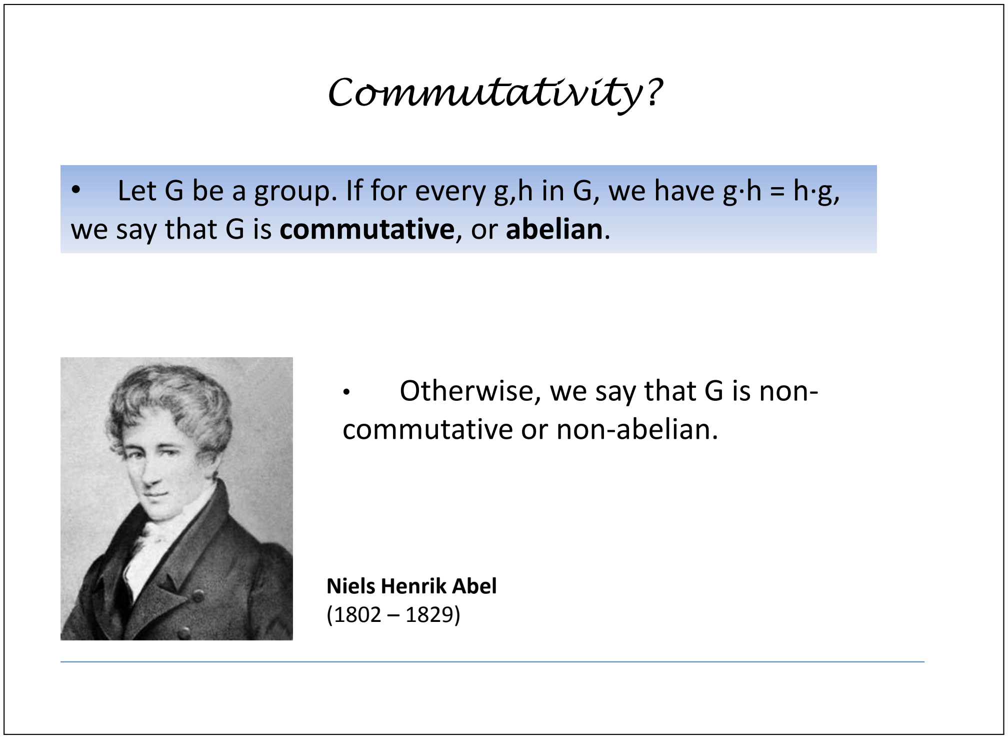
Because e is an identity element, we have

$$e \cdot e' = e'.$$

Because e’ is also an identity element, we have

$$e \cdot e' = e.$$

Hence $e \cdot e' = e' = e$, which concludes the proof.



Commutativity?

- Let G be a group. If for every g,h in G, we have $g \cdot h = h \cdot g$, we say that G is **commutative**, or **abelian**.

- Otherwise, we say that G is non-commutative or non-abelian.

Niels Henrik Abel
(1802 – 1829)

Suppose we have a group with a given binary operation. We now look at subsets of this group, which also have a group structure with respect to the same binary operation!

Definition 6. If $(G, \cdot)$ is a group and H is a subset of G, so that $(H, \cdot)$ is a group too, we shall call $(H, \cdot)$ a subgroup of G.

Note again that the above definition can be written in additive notation.

We may consider the subgroup $H = G$ as a subgroup of G. Another example of subgroup which is always present in any group G is the *trivial* subgroup formed by the identity element only!

Let us use the multiplicative notation, and let $(G, \cdot)$ be a group with identity element 1. Now we need to check that $H = \{1\}$ is indeed a subgroup of G. It is of course a subset of G, so we are left to check that it has a group structure. Well, all we need to know here is that $1 \cdot 1 = 1$, which is true from the fact that G is a group. This shows at once that (1) combining elements of H gives an element in H, (2) there is an identity element in H, and (3) the element of H is invertible (it is its own inverse in fact). There is no need to check the associativity of the binary law here, since it is inherited from that of G.

If H is a subgroup of G, they are both groups, and the size of H is always smaller or equal to that of G. The size of a group G has a name, we usually refer to it as being the order of the group G.

Definition 7. If $(G, \cdot)$ is a group, the number of elements of G (i.e., the cardinality of the set G) is called the order of the group G. It is denoted by $|G|$.

For example, to write formally that the size of a subgroup H of G is always smaller or equal to that of G, we write: $|H| \leq |G|$.

A group G can be finite ($|G| < \infty$) or infinite ($|G| = \infty$)! We will see examples of both types.

Be careful here: the word “order” means *two different things*
in group theory, depending on whether we refer to the order of a group,
or to the order of an element!!

We next define the order of an element in a group.

A Group inside a Group

- If G is a group, and H is a subset of G which is a group with respect to the binary operation of G, then H is called a **subgroup** of G.

(H =G is a subgroup of G.)

The trivial Group

- The set containing only the identity element is a group, sometimes called the trivial group.
- It is denoted by
  - {0} (additive notation)
  - {1} (multiplicative notation) .
- Every group contains the trivial group as a subgroup.

From now on, we will adopt the multiplicative notation, and very often when things are clear enough even remove the $\cdot$ notation. For example, we will write $g_1 g_2$ instead of $g_1 \cdot g_2$.

Definition 8. Let G be a group with identity element e. The order of an element g in G is the **smallest positive integer** k such that

$$\underbrace{ggg\cdots g}_{k\ times} = g^k = e.$$

Note that such a k might not exist! In that case, we will say that g has an infinite order. The notation for the order of an element g varies, it is sometimes denoted by $|g|$, or $o(g)$.

One might wonder why we have two concepts of order, with the same name. It suggests they might be related, and in fact they are, but this is something we will see only later!

Let $(G, \cdot)$ be a group whose order is $|G| = n$, that is G contains a finite number n of elements. Suppose that this group G contains an element g whose order is also n, that is an element g such that

$$g^n = e$$

and there is no smaller positive power k of g such that $g^k = e$. Then

$$g, g^2, \ldots, g^{n-1}, g^n = e$$

are all distinct elements of G. Indeed should we have some $g^s = g^{s+t}$ for $t < n$ then by multiplying both sides with g^{-s}, we would get that $g^t = 1$ for $t < n$, a contradiction to the minimality of n!

But the group, by assumption, has only n distinct elements, hence we must have that

$$G = \{1, g, g^2, \ldots, g^{n-1}\}.$$

If this is the case, we say that $(G, \cdot)$ is **generated** by g, which we write $G = \langle g \rangle$.

These types of groups are very nice! In fact they are the simplest form of groups that we will encounter. They are called cyclic groups.

Order of a Group/Order of an Element

The cardinality of a group G is called the **order of G** and is denoted by |G|.

- A group can be finite or infinite.

The **order of an element g in G** is the **smallest** positive integer k such that $g^k=1$. If no such k exist, the order is ∞.

- Does having the same name mean that there is a link between the order of a group and order of an element?
- Actually yes….but not so easy to see…

When order of element = order of group

- Let G be a group of finite order n (|G|=n).
- What happens if there exists an element g in the group G such that the order of g =n?
- This means $g^n=1$, and there is no k>0 smaller such that $g^k=1$.
- This means that G is exactly described by $G=\{1,g,g^2,g^3,\dots,g^{n-1}\}$.
- In this case, we say that G is a **cyclic group**.

Definition 9. A group G will be called cyclic if it is generated by an element g of G, i.e.,

$$G = \langle g \rangle = \{g^m | m \in \mathbb{Z}\}.$$

Notice that this definition covers both the case of a finite cyclic group (in that case, $g^n = e$ for some n, and this set is indeed finite) and of an infinite cyclic group.

To start with, cyclic groups have this nice property of being abelian groups.

Proposition 2. *Cyclic groups are abelian.*

Proof. To show that a group is abelian, we have to show that

$$g_1 g_2 = g_2 g_1$$

for any choice of elements g_1 and g_2 in G. Now let G be a cyclic group. By definition, we know that G is generated by a single element g, that is

$$G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}.$$

Thus both g_1 and g_2 can be written as a power of g:

$$g_1 = g^i, \ g_2 = g^j$$

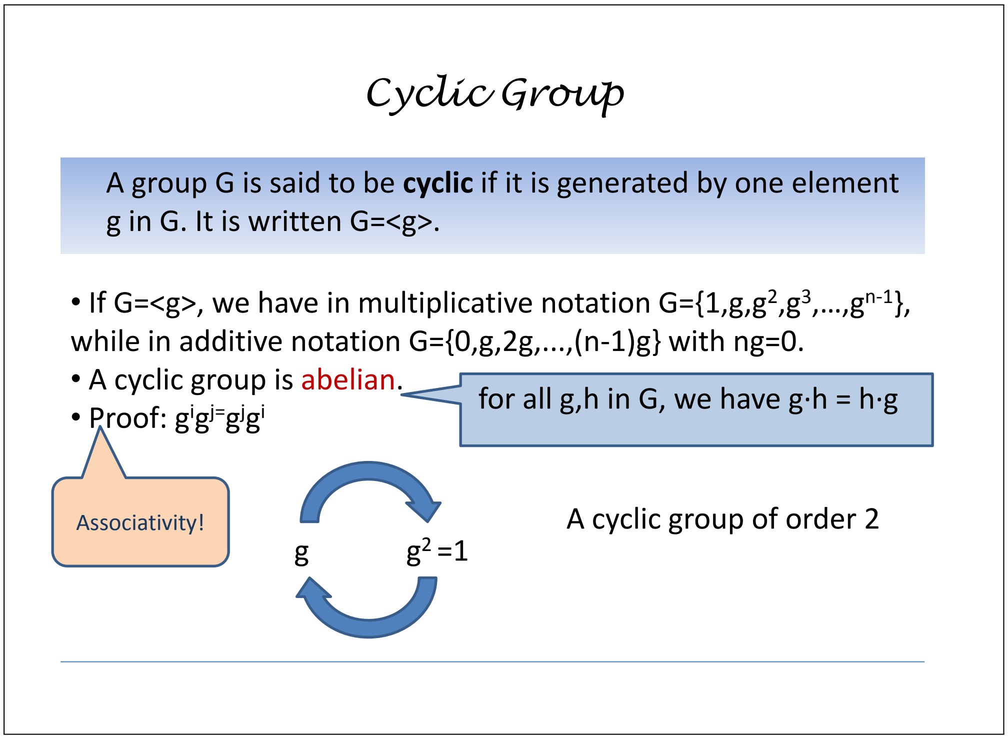
for some power i and j, and thus, thanks to the associativity of the binary operation

$$g_1 g_2 = g^i g^j = g^{i+j} = g^j g^i = g_2 g_1$$

which concludes the proof. □

Let us summarize what we have been doing so far in this chapter.

- We defined this abstract notion of group.
- Using it, we defined more abstract things: an abelian group, the order of a group, the order of an element of a group, the notion of subgroup, and that of cyclic group.
- We also saw that based only on these definitions, we can start proving results, such as the uniqueness of the identity element, or the fact that cyclic groups are abelian.



Cyclic Group

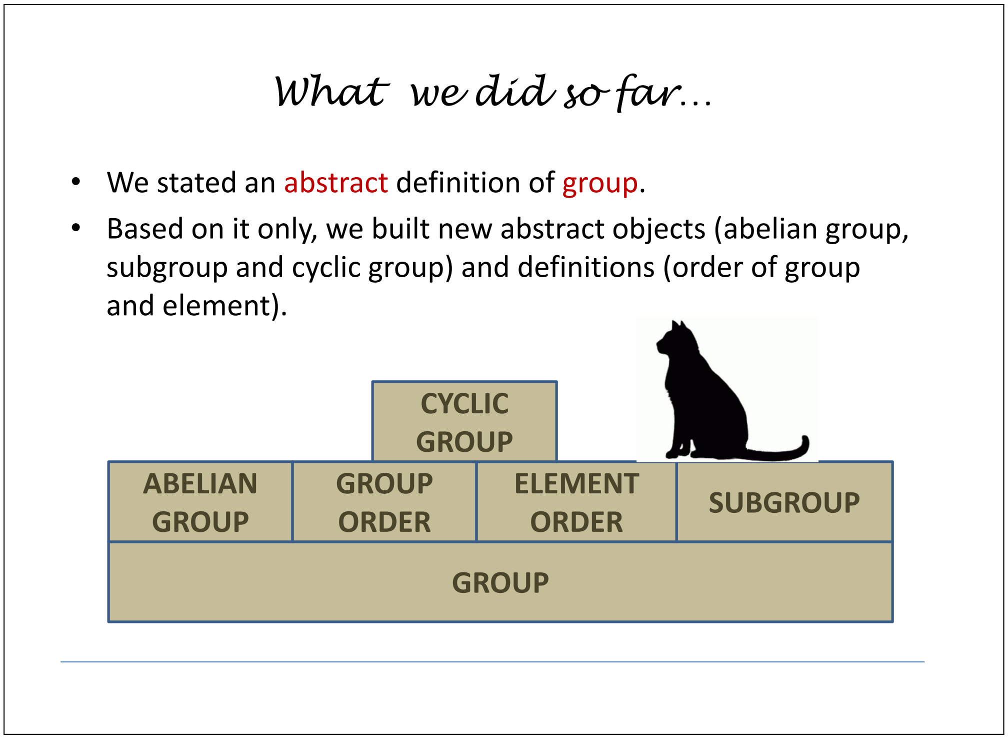
A group G is said to be **cyclic** if it is generated by one element g in G. It is written G=<g>.

- If G=<g>, we have in multiplicative notation G={1,g,g^2,g^3,…,g^{n-1}}, while in additive notation G={0,g,2g,…,(n-1)g} with ng=0.
- A cyclic group is abelian.
- Proof: $g^i g^j = g^j g^i$

for all g,h in G, we have g·h = h·g

Associativity!

A cyclic group of order 2



What we did so far…

- We stated an abstract definition of group.
- Based on it only, we built new abstract objects (abelian group, subgroup and cyclic group) and definitions (order of group and element).

CYCLIC GROUP
ABELIAN GROUP
GROUP ORDER
ELEMENT ORDER
SUBGROUP
GROUP

This might look really abstract, which is somewhat normal since this is a first step into abstract algebra. However, you already know all these abstract objects, because you saw them already in the two previous chapters! These definitions are abstracting mathematical properties that we observed. We will spend the rest of this chapter to convince you that this is indeed the case.

We will use a lot the notion of multiplication table for the rest of this chapter. We note that they are sometimes called *Cayley tables*.

Recall from the previous chapter that we have obtained the complete set of symmetries for a rectangle, whose multiplication table we recall below (we write $m = m_v$ for the vertical mirror reflection):

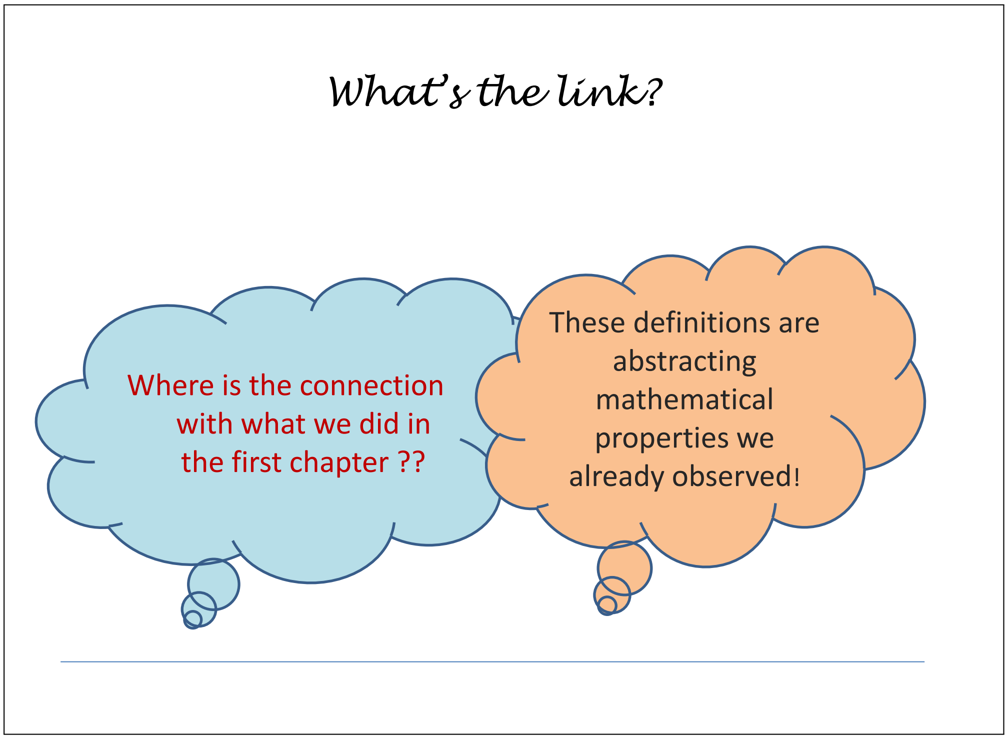
	1	m	r_π	mr_π
1	1	m	r_π	mr_π
m	m	1	mr_π	r_π
r_π	r_π	mr_π	1	m
mr_π	mr_π	r_π	m	1

First of all, let us see that the symmetries of a rectangle form a group G, with respect to the binary operation given by the composition of maps.

- Composition of symmetries yields another symmetry (this can be observed from the multiplication table).
- Composition of symmetries is associative.
- There exists an identity element, the identity map 1.
- Each element has an inverse (itself!) This can be seen from the table as well!

This shows that the set of symmetries of a rectangle forms a group. Note that this group is abelian, which can be seen from the fact that the multiplication table is symmetric w.r.t. the main diagonal.

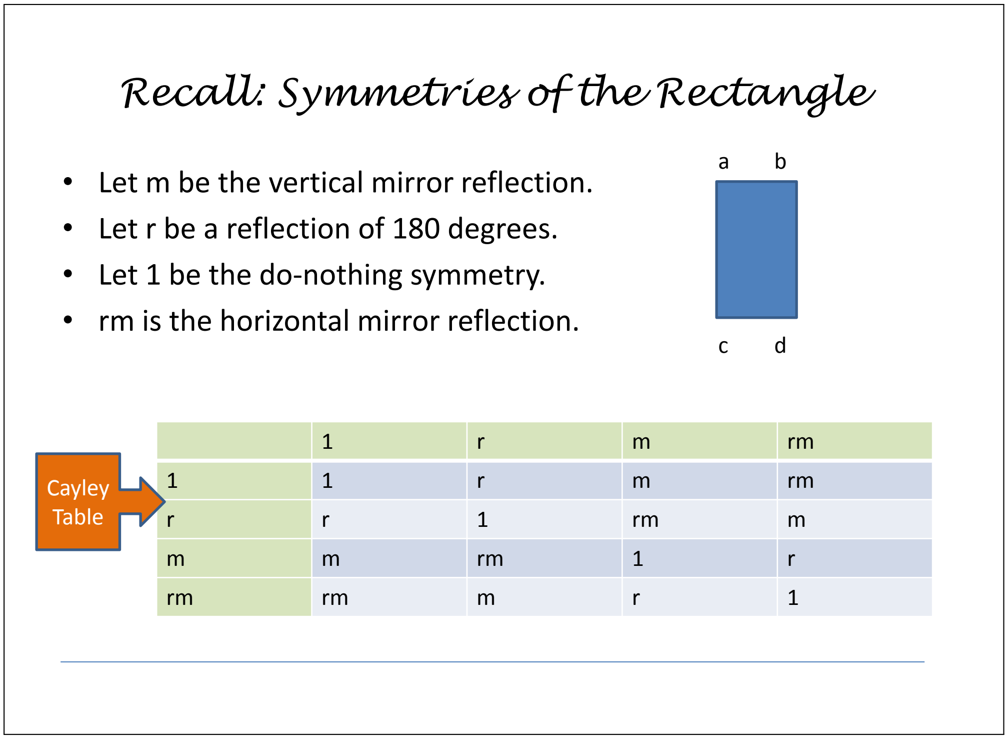
Of course, that the set of symmetries of a rectangle forms an abelian group can be shown without computing a multiplication table, but since we know it, it gives an easy way to visualize the group structure.



What's the link?

Where is the connection with what we did in the first chapter ??

These definitions are abstracting mathematical properties we already observed!



Recall: Symmetries of the Rectangle

- Let m be the vertical mirror reflection.
- Let r be a reflection of 180 degrees.
- Let 1 be the do-nothing symmetry.
- rm is the horizontal mirror reflection.

Cayley Table

	1	r	m	rm
1	1	r	m	rm
r	r	1	rm	m
m	m	rm	1	r
rm	rm	m	r	1

The group of symmetries of the rectangle has order 4.

Let us look at the order of the elements:

$$m^2 = 1,\ r^2 = 1,\ (rm)^2 = 1,$$

thus these elements have order 2.

We next look at the subgroups:

- The trivial subgroup $\{1\}$ is here.
- We have that $\{1, r\}$ forms a subgroup of order 2.
- Similarly $\{1, m\}$ forms a subgroup of order 2.
- Finally $\{1, rm\}$ also forms a subgroup of order 2.

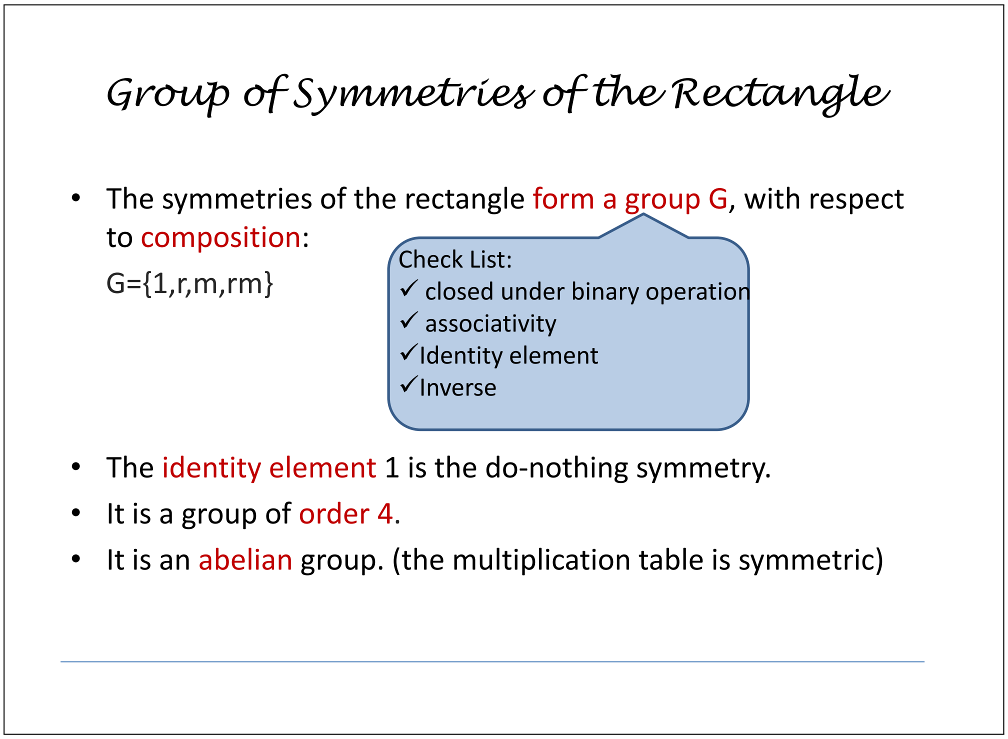
We can observe that these are the only subgroups, since by adding a 3rd element to any of them, we will get the whole group! Let us illustrate this claim with an example. Let us try to add to $\{1, r\}$, say m. We get $H = \{1, r, m\}$ but for this set H to be a group, we need to make sure that the composition of any two maps is in H! Clearly rm is not, so we need to add it if we want to get a group, but then we get G!

We further note that all the subgroups are cyclic subgroups! For example, $\{1, m\} = \langle m \rangle$. But G itself is not a cyclic group, since it contains no element of order 4.

Let us summarize our findings:

Let G be the group of symmetries of the rectangle.

1. It is an **abelian** group of **order 4**.
2. Apart from the identity element, it contains 3 elements of order 2.
3. It is **not a cyclic** group.
4. It contains 3 cyclic subgroups of order 2.



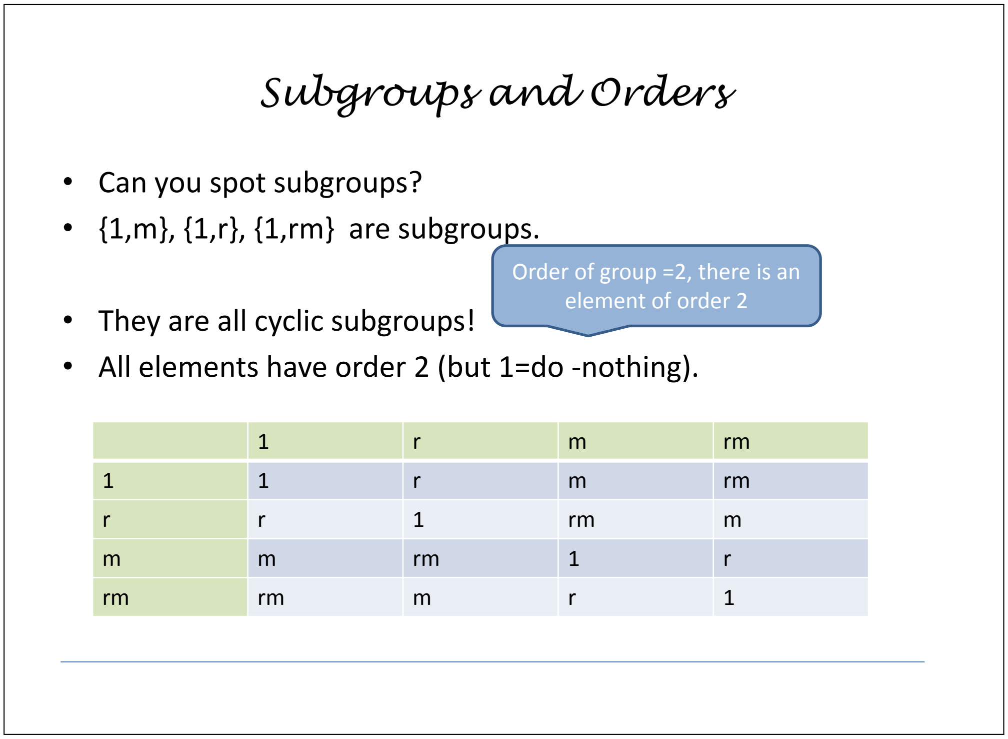
Group of Symmetries of the Rectangle

- The symmetries of the rectangle form a group G, with respect to composition:

  G={1,r,m,rm}

Check List:
✓ closed under binary operation
✓ associativity
✓ Identity element
✓ Inverse

- The identity element 1 is the do-nothing symmetry.
- It is a group of order 4.
- It is an abelian group. (the multiplication table is symmetric)



Subgroups and Orders

- Can you spot subgroups?
- {1,m}, {1,r}, {1,rm} are subgroups.

Order of group =2, there is an element of order 2

- They are all cyclic subgroups!
- All elements have order 2 (but 1=do -nothing).

	1	r	m	rm
1	1	r	m	rm
r	r	1	rm	m
m	m	rm	1	r
rm	rm	m	r	1

Let us now look at our second example, the symmetries of the square. We recall that there are 8 symmetries:

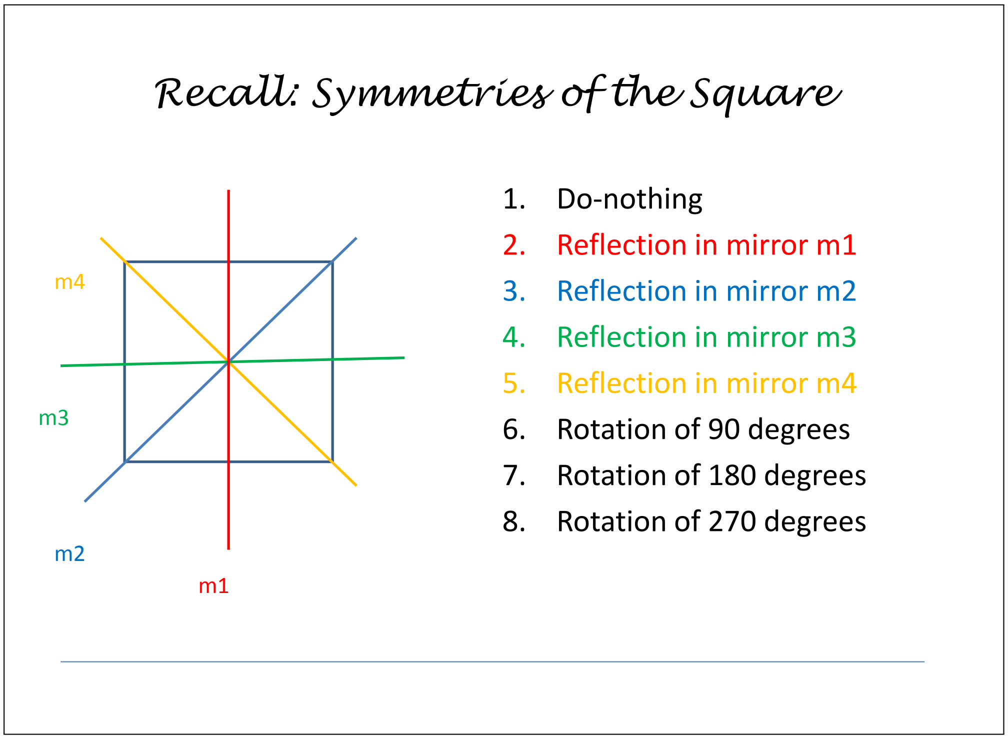
1. m_1= reflection with respect to the y-axis,
2. m_2= reflection with respect to the line $y = x$,
3. m_3= reflection with respect to the x-axis,
4. m_4= reflection with respect to the line $y = -x$,
5. the rotation $r_{\pi/2}$,
6. the rotation r_π,
7. the rotation $r_{3\pi/2}$,
8. and of course the identity map 1!

By fixing $m = m_3$ and $r = r_{3\pi/2}$, we also computed that

$$\begin{aligned} rm &= m_4 \\ r^2m &= m_1 \\ r^3m &= m_2 \end{aligned}$$

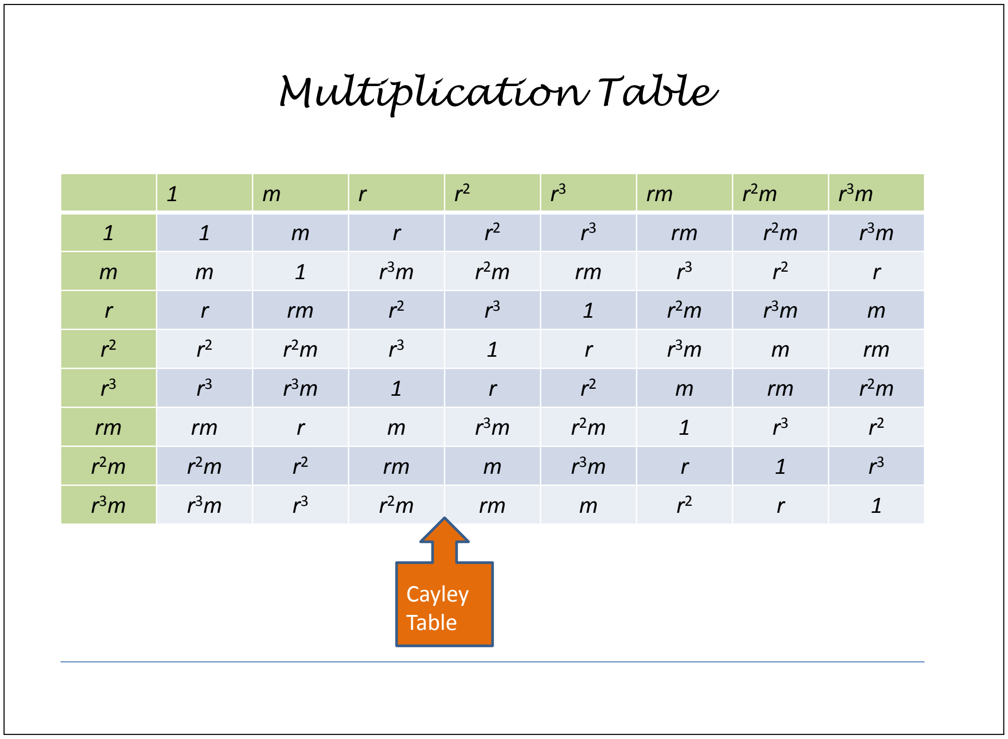
which allowed us to compute the following multiplication (Cayley) table.

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1



Recall: Symmetries of the Square

1. Do-nothing
2. Reflection in mirror m1
3. Reflection in mirror m2
4. Reflection in mirror m3
5. Reflection in mirror m4
6. Rotation of 90 degrees
7. Rotation of 180 degrees
8. Rotation of 270 degrees



Multiplication Table

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1

Cayley Table

Let us check that the symmetries of the square form a group. We consider the set

$$G = \{1, r, r^2, r^3, m, mr, mr^2, mr^3\}$$

together with the composition of maps as binary law. Then we have

- closure under the binary composition, that is the composition of two symmetries is again a symmetry,
- the composition is associative,
- there exists an identity element,
- each element has an inverse (this can be seen in the table, since every row has a 1!)

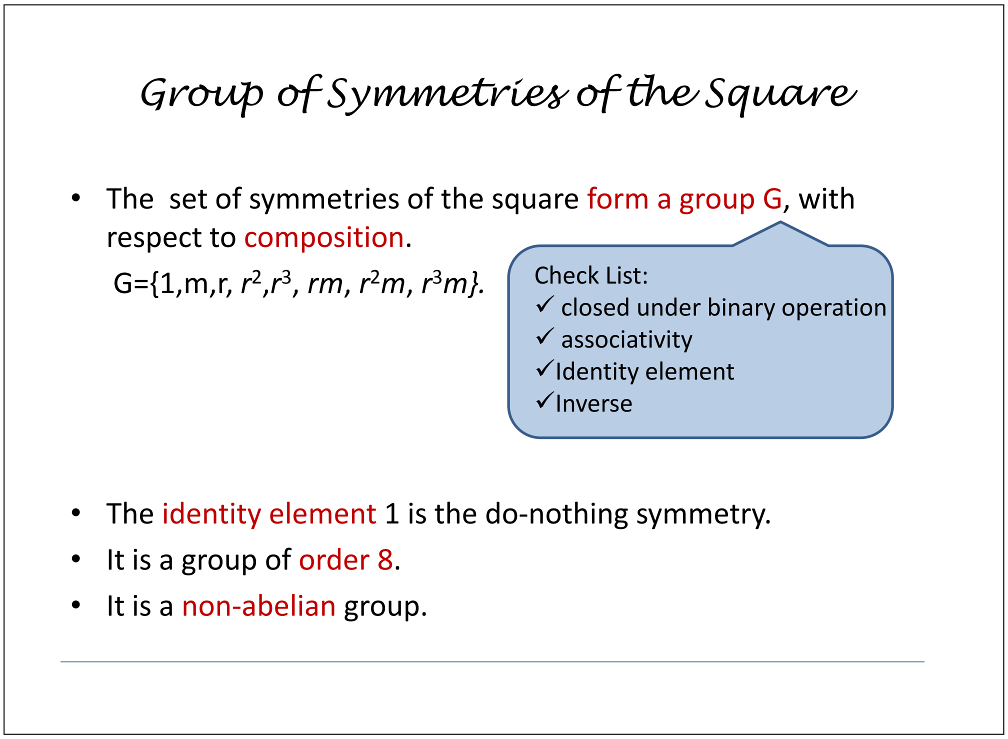
We just showed that G is a group.

It is a group of order 8, which is not abelian, since $rm \neq mr$. Note that as a result G cannot be cyclic, since we proved that every cyclic group is abelian!

We next look at possible subgroups of G. Let us try to spot some of them.

- We have that $\{1, m\}$ forms a subgroup of order 2. It contains an element m of order 2, thus it is cyclic!
- Another subgroup can be easily spotted by reordering the rows and columns of the Cayley table. This is $\{1, r, r^2, r^3\}$, which is a subgroup of order 4. It contains one element of order 4, that is r, and thus it is cyclic as well! It also contains one element of order 2, that is r^2. The element r^3 also has order 4.
- The subgroup $\{1, r, r^2, r^3\}$ itself contains another subgroup of order 2, given by $\{1, r^2\}$, which is cyclic of order 2.

We have now spotted the most obvious subgroups, let us see if we missed something.



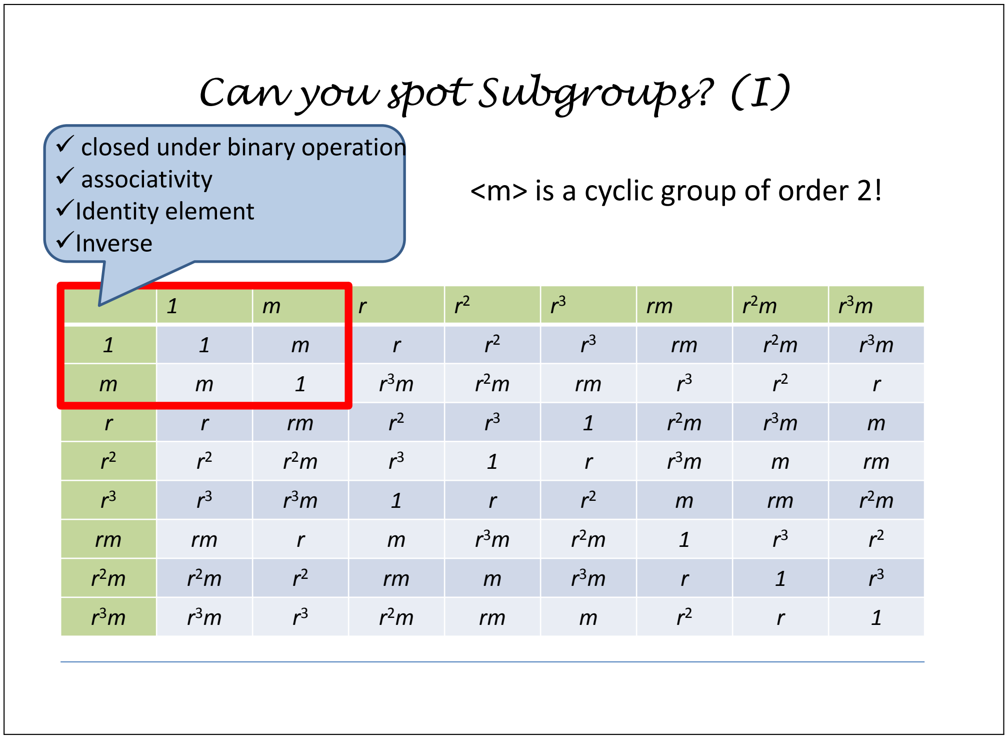
Group of Symmetries of the Square

- The set of symmetries of the square form a group G, with respect to composition.

  G={1,m,r, r^2,r^3, rm, r^2m, r^3m}.

Check List:
✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse

- The identity element 1 is the do-nothing symmetry.
- It is a group of order 8.
- It is a non-abelian group.



Can you spot Subgroups? (I)

✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse

<m> is a cyclic group of order 2!

	1	m	r	r^2	r^3	rm	r^2m	r^3m
1	1	m	r	r^2	r^3	rm	r^2m	r^3m
m	m	1	r^3m	r^2m	rm	r^3	r^2	r
r	r	rm	r^2	r^3	1	r^2m	r^3m	m
r^2	r^2	r^2m	r^3	1	r	r^3m	m	rm
r^3	r^3	r^3m	1	r	r^2	m	rm	r^2m
rm	rm	r	m	r^3m	r^2m	1	r^3	r^2
r^2m	r^2m	r^2	rm	m	r^3m	r	1	r^3
r^3m	r^3m	r^3	r^2m	rm	m	r^2	r	1

If we take the subgroup $\{1, r, r^2, r^3\}$ and try to add one more element, say m, we realize that rm, r^2m,... must be there as well, and thus we get the whole group G.

Let us try to add some more elements to the subgroup $\{1, m\}$. If we add r, then we need to add all the power of r, and we obtain the whole group G again.

Alternatively we could try to add r^2 to $\{1, m\}$. Then we get $H = \{1, m, r^2, r^2m, mr^2\}$, and this we have that $r^2m = mr^2$. Thus we managed to find another subgroup, this time of order 4. It contains 3 elements of order 2.

We had identified the subgroup $\{1, r^2\}$. If we add m, we find the subgroup H again. If we add rm, we find another subgroup given by $\{1, r^2, rm, r^3m\}$.

Finally, we had mentioned at the beginning that $\{1, m\}$ forms a subgroup of order 2. But this is true for every mirror reflection, and we have more than one such reflection: we know we have 4 of them! Thus to each of them corresponds a cyclic subgroup of order 2.

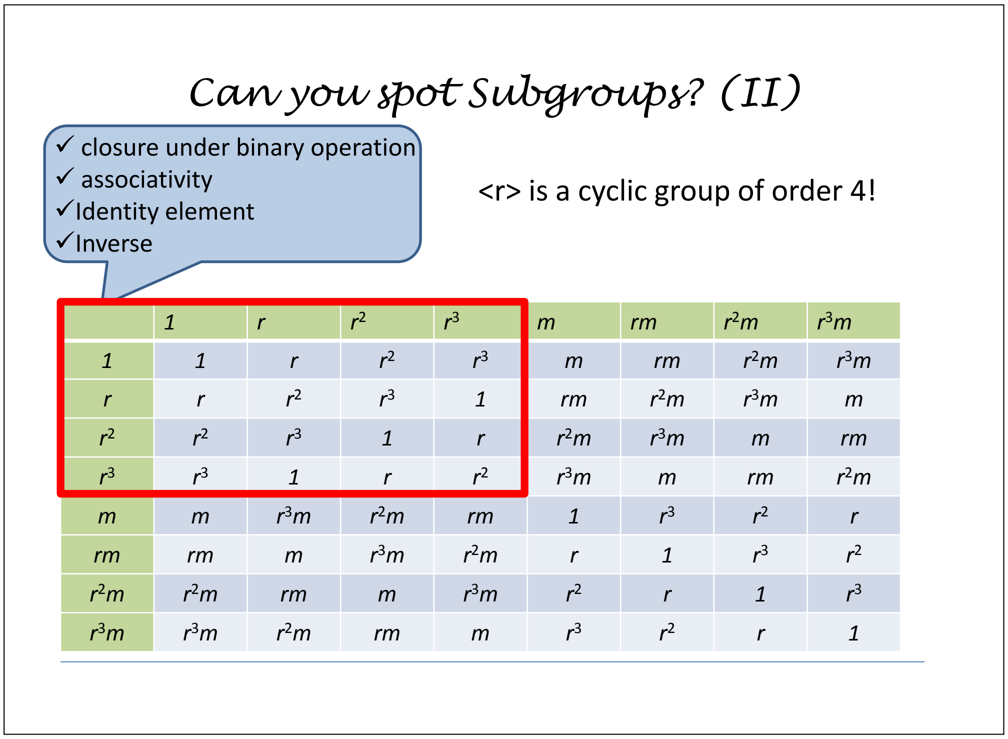
We list all the subgroups of G that we found.

Let G be the group of symmetries of the square. Here is a list of its subgroups.

1. Order 1: the trivial subgroup $\{1\}$.
2. Order 2: the cyclic groups generated by the 4 reflections, that is $\{1, m\}$, $\{1, rm\}$, $\{1, r^2m\}$ and $\{1, r^3m\}$, together with $\{1, r^2\}$.
3. Order 4: we have $\{1, r, r^2, r^3\}$ which is cyclic, and $\{1, m, r^2, r^2m, mr^2\}$ together with $\{1, r^2, rm, r^3m\}$ which are not cyclic.

It is interesting to recognize the group of symmetries of the rectangle, which makes sense, since a square is a special rectangle.

You are right to think that finding all these subgroups is tedious! In fact, finding the list of all subgroups of a given group in general is really hard. However there is nothing to worry about here, since we will not try for bigger groups, and for the symmetries of the square, it was still manageable.

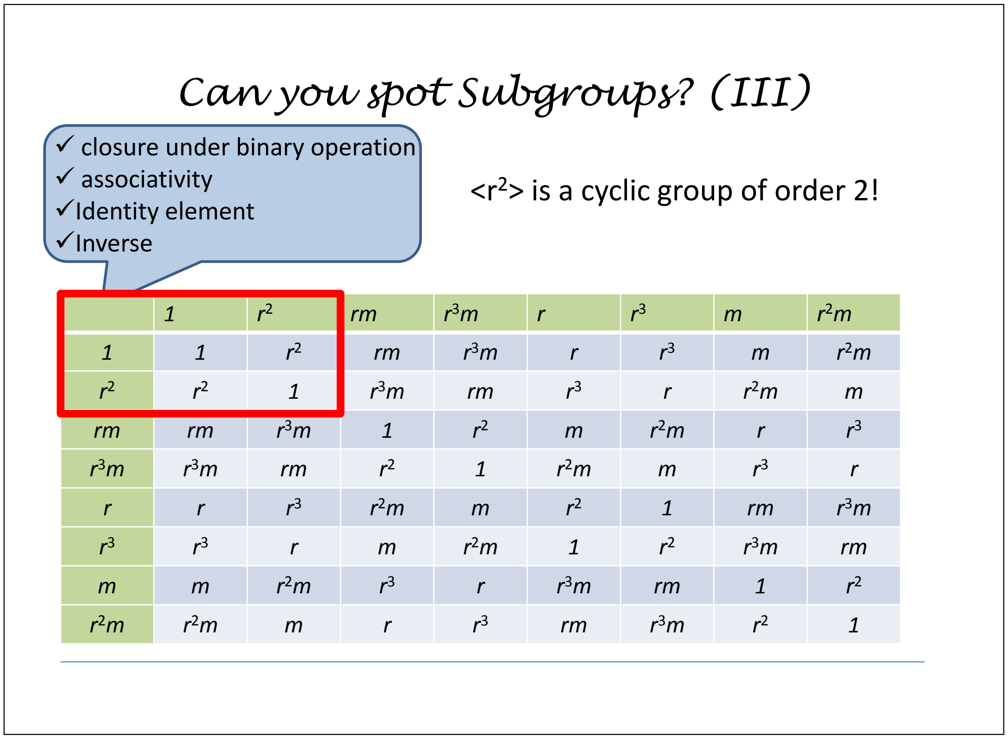


Can you spot Subgroups? (II)

- ✓ closure under binary operation
- ✓ associativity
- ✓ Identity element
- ✓ Inverse

<r> is a cyclic group of order 4!

	1	r	r^2	r^3	m	rm	r^2m	r^3m
1	1	r	r^2	r^3	m	rm	r^2m	r^3m
r	r	r^2	r^3	1	rm	r^2m	r^3m	m
r^2	r^2	r^3	1	r	r^2m	r^3m	m	rm
r^3	r^3	1	r	r^2	r^3m	m	rm	r^2m
m	m	r^3m	r^2m	rm	1	r^3	r^2	r
rm	rm	m	r^3m	r^2m	r	1	r^3	r^2
r^2m	r^2m	rm	m	r^3m	r^2	r	1	r^3
r^3m	r^3m	r^2m	rm	m	r^3	r^2	r	1



Can you spot Subgroups? (III)

- ✓ closure under binary operation
- ✓ associativity
- ✓ Identity element
- ✓ Inverse

<r^2> is a cyclic group of order 2!

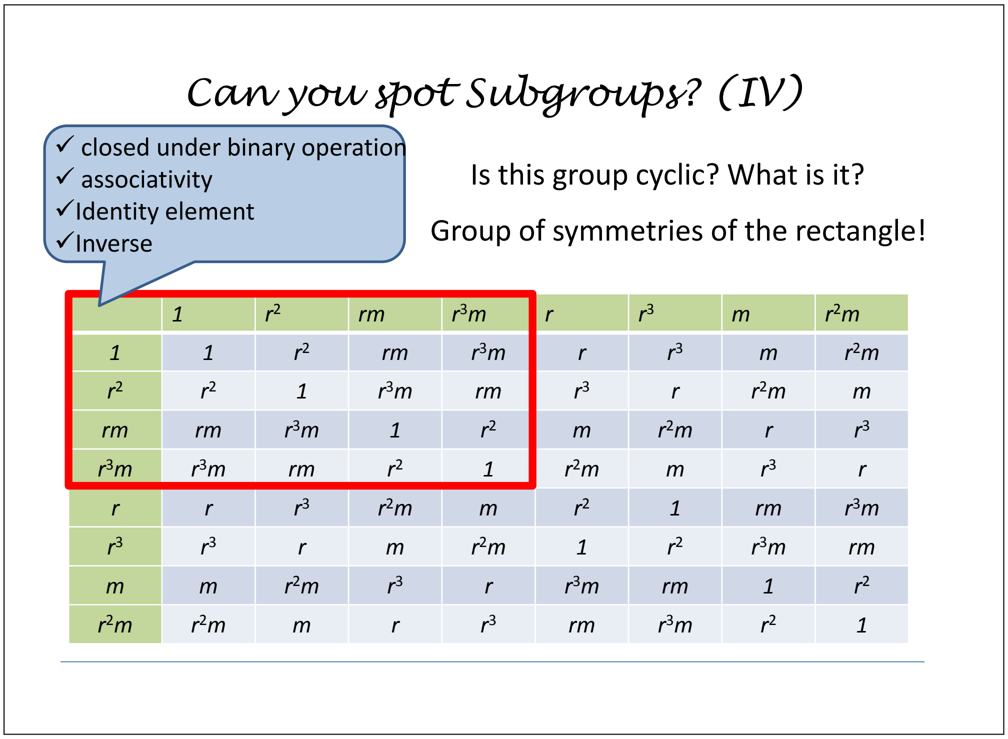
	1	r^2	rm	r^3m	r	r^3	m	r^2m
1	1	r^2	rm	r^3m	r	r^3	m	r^2m
r^2	r^2	1	r^3m	rm	r^3	r	r^2m	m
rm	rm	r^3m	1	r^2	m	r^2m	r	r^3
r^3m	r^3m	rm	r^2	1	r^2m	m	r^3	r
r	r	r^3	r^2m	m	r^2	1	rm	r^3m
r^3	r^3	r	m	r^2m	1	r^2	r^3m	rm
m	m	r^2m	r^3	r	r^3m	rm	1	r^2
r^2m	r^2m	m	r	r^3	rm	r^3m	r^2	1

We finish this example by summarizing all that we found about the group of symmetries of the square.

Let G be the group of symmetries of the square.

1. It is a group of **order 8**.
2. Apart from the identity element, it contains 7 elements, 5 of order 2, and 2 of order 4.
3. It is **not a cyclic** group.
4. In fact, it is **not even an abelian** group.
5. It contains 5 cyclic subgroups of order 2, 1 cyclic subgroup of order 4, and 2 subgroups of order 4 which are not cyclic, for a total of 8 non-trivial subgroups.

In the first two chapters, we explained mathematically nice geometric structures using the notion of symmetries. What we saw in this chapter is that symmetries in fact have a nice algebraic structure, that of a group. What we will do next is study more about groups! Once we have learnt more, we will come back to symmetries again, and see that we can get a much better understanding thanks to some group theory knowledge.



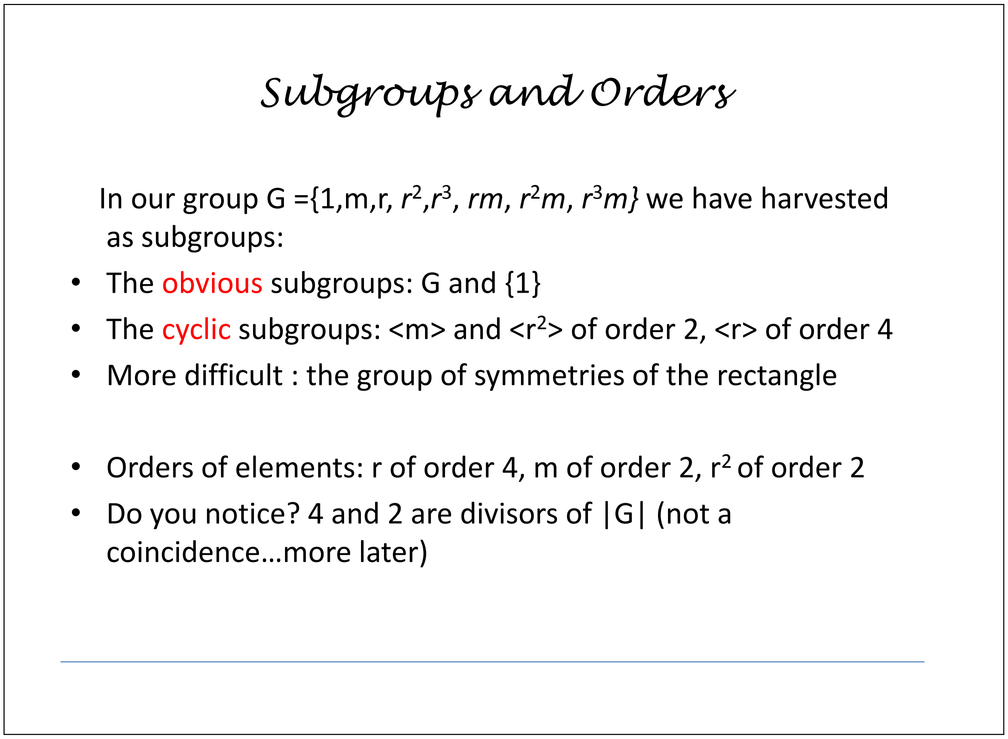
Can you spot Subgroups? (IV)

✓ closed under binary operation
✓ associativity
✓Identity element
✓Inverse

Is this group cyclic? What is it?

Group of symmetries of the rectangle!

	1	r^2	rm	r^3m	r	r^3	m	r^2m
1	1	r^2	rm	r^3m	r	r^3	m	r^2m
r^2	r^2	1	r^3m	rm	r^3	r	r^2m	m
rm	rm	r^3m	1	r^2	m	r^2m	r	r^3
r^3m	r^3m	rm	r^2	1	r^2m	m	r^3	r
r	r	r^3	r^2m	m	r^2	1	rm	r^3m
r^3	r^3	r	m	r^2m	1	r^2	r^3m	rm
m	m	r^2m	r^3	r	r^3m	rm	1	r^2
r^2m	r^2m	m	r	r^3	rm	r^3m	r^2	1



Subgroups and Orders

In our group G ={1,m,r, r^2,r^3, rm, r^2m, r^3m} we have harvested as subgroups:

- The obvious subgroups: G and {1}
- The cyclic subgroups: <m> and <r^2> of order 2, <r> of order 4
- More difficult : the group of symmetries of the rectangle

- Orders of elements: r of order 4, m of order 2, r^2 of order 2
- Do you notice? 4 and 2 are divisors of |G| (not a coincidence…more later)

Exercises for Chapter 3

Exercise 11. In Exercise 7, you determined the symmetries of an equilateral triangle, and computed the multiplication table of all its symmetries. Show that the symmetries of an equilateral triangle form a group.

1. Is it abelian or non-abelian?
2. What is the order of this group?
3. Compute the order of its elements.
4. Is this group cyclic?
5. Can you spot some of its subgroups?

Exercise 12. Let $z = e^{2i\pi/3}$. Show that $\{1, z, z^2\}$ forms a group.

1. Is it abelian or non-abelian?
2. What is the order of this group?
3. Compute the order of its elements.
4. Is this group cyclic?
5. Can you spot some of its subgroups?

Exercise 13. Let X be a metric space equipped with a distance d.

1. Show that the set of bijective isometries of X (with respect to the distance d) forms a group denoted by G.
2. Let S be a subset of X. Define a symmetry f of S as a bijective isometry of X that maps S onto itself (that is $f(S) = S$). Show that the set of symmetries of S is a subgroup of G.

Exercise 14. Let G be a group. Show that right and left cancellation laws hold (with respect to the binary group operation), namely:

$$g_2 \cdot g_1 = g_3 \cdot g_1 \Rightarrow g_2 = g_3,$$

$$g_3 \cdot g_1 = g_3 \cdot g_2 \Rightarrow g_1 = g_2,$$

for any $g_1, g_2, g_3 \in G$.

Exercise 15. Let G be an abelian group. Is the set

$$\{x \in G,\ x = x^{-1}\}$$

a subgroup of G? Justify your answer.

Exercise 16. Let G be a group, and let H be a subgroup of G. Consider the set

$$gH = \{gh,\ h \in H\}.$$

1. Show that $|gH| = |H|$.
2. Is thet set

   $$\{g \in G,\ gH = Hg\}$$

   a subgroup of G?

Exercise 17. Let G be a group, show that

$$(g_1g_2)^{-1} = g_2^{-1}g_1^{-1},$$

for every $g_1, g_2 \in G$. This is sometimes called the "shoes and socks property"!

Exercise 18. In a finite group G, every element has finite order. True or false? Justify your answer.

Exercise 19. This exercise is to practice Cayley tables.

1. Suppose that G is a group of order 2. Compute its Cayley table.

   Guided version.

   - Since G is of order 2, this means it has two elements, say $G = \{g_1, g_2\}$. Decide a binary law, say a binary law that is written multiplicatively.
   - Now use the definition of group to identify that one of the two elements must be an identity element 1. Then write the Cayley table.
   - Once you have written all the elements in the table, make sure that this table is indeed that of group! (namely make sure that you used the fact that every element is invertible).

2. Suppose that G is a group of order 3. Compute its Cayley table.

Exercise 20. Consider the set $M_n(\mathbb{R})$ of $n \times n$ matrices with coefficients in $\mathbb{R}$. For this exercise, you may assume that matrix addition and multiplication is associative.

1. Show that $M_n(\mathbb{R})$ is a group under addition.

2. Explain why $M_n(\mathbb{R})$ is not a group under multiplication.

3. Let $GL_n(\mathbb{R})$ be the subset of $M_n(\mathbb{R})$ consisting of all invertible matrices. Show that $GL_n(\mathbb{R})$ is a multiplicative group. ($GL_n(\mathbb{R})$ is called a *General Linear group*).

4. Let $SL_n(\mathbb{R})$ be the subset of $GL_n(\mathbb{R})$ consisting of all matrices with determinant 1. Show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. ($SL_n(\mathbb{R})$ is called a *Special Linear group*).

5. Explain whether $SL_n(\mathbb{R})$ is a subgroup of $M_n(\mathbb{R})$

Chapter 4

The Group Zoo

> *"The universe is an enormous direct product of representations of symmetry groups." (Hermann Weyl, mathematician)*

In the previous chapter, we introduced *groups* (together with subgroups, order of a group, order of an element, abelian and cyclic groups) and saw as examples the group of symmetries of the square and of the rectangle. The concept of group in mathematics is actually useful in a variety of areas beyond geometry and sets of geometric transformation. We shall next consider many sets endowed with binary operations yielding group structures. We start with possibly the most natural example, that of real numbers. Since both addition and multiplication are possible operations over the reals, we need to distinguish with respect to which we are considering a group structure.

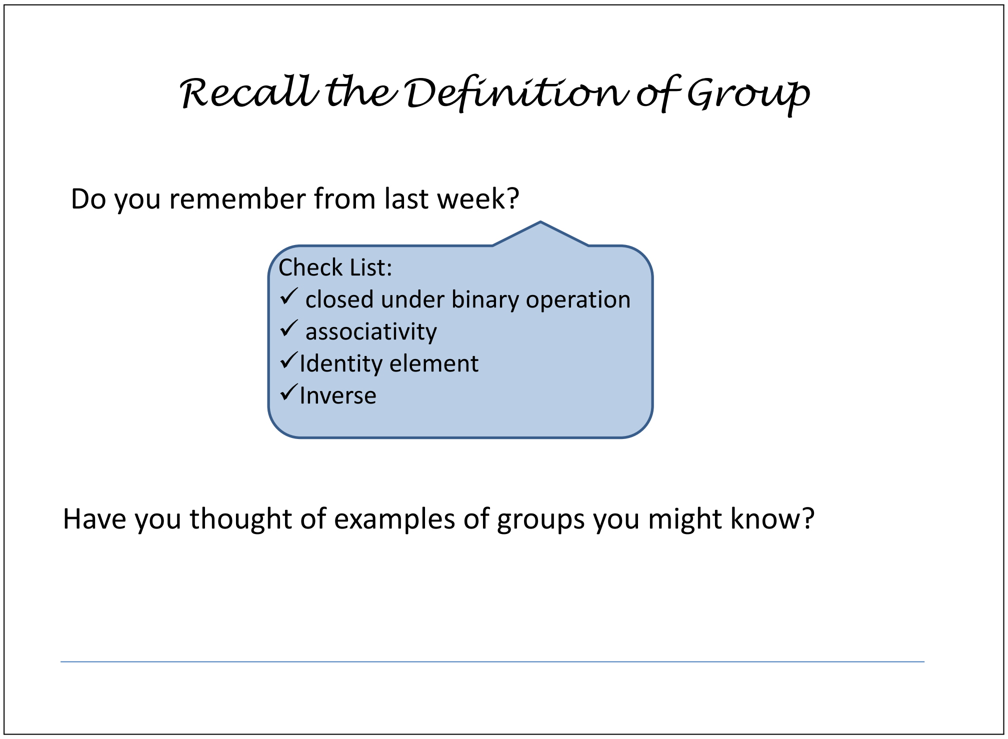
Example 1. We have that $(\mathbb{R}, +)$ is a group.

- $\mathbb{R}$ is closed under addition, which is associative.
- $\forall x \in \mathbb{R}, x + 0 = 0 + x = x$, hence 0 is the identity element.
- $\forall x \in \mathbb{R}, \exists (-x) \in \mathbb{R}$, so that $x + (-x) = 0$.

Example 2. We have that $(\mathbb{R}^*, \cdot)$, where $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$, forms a group:

- $\mathbb{R}^*$ is closed under multiplication, which is associative.
- $\forall x \in \mathbb{R}^*$, $x \cdot 1 = 1 \cdot x = x$, hence 1 is the identity element.
- $\forall x \in \mathbb{R}^*, \exists x^{-1} = \frac{1}{x}$, so that $x \cdot (\frac{1}{x}) = (\frac{1}{x}) \cdot x = 1$.

Both $(\mathbb{R}, +)$ and $(\mathbb{R}^*, \cdot)$ are abelian groups, of infinite order ($|\mathbb{R}| = \infty$, $|\mathbb{R}^*| = \infty$).

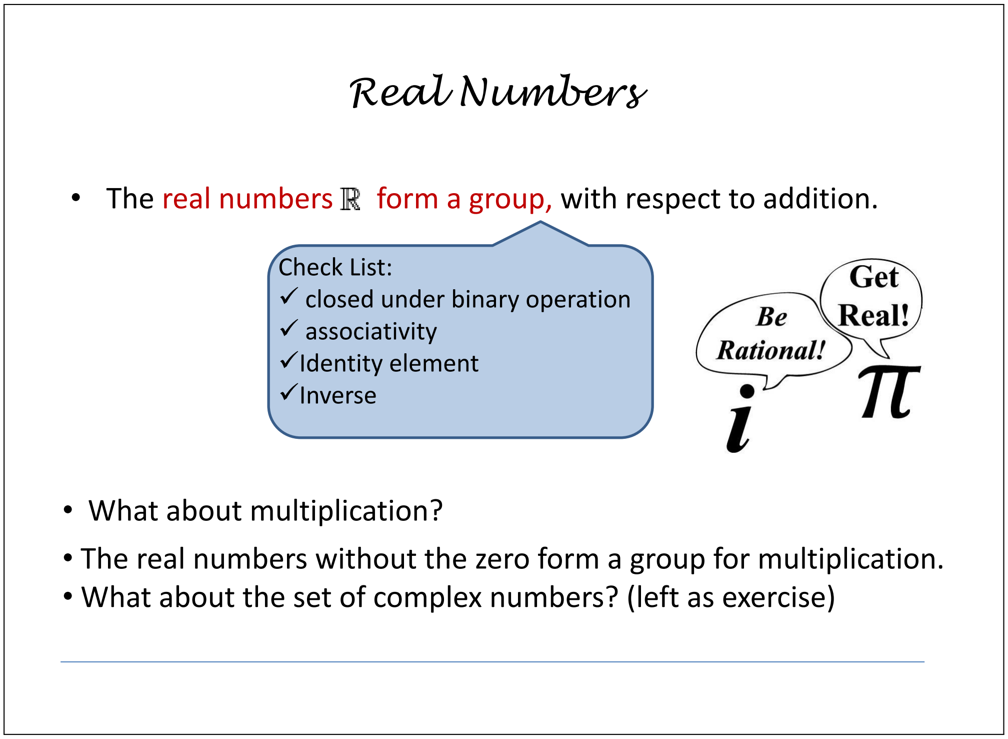


Recall the Definition of Group

Do you remember from last week?

Check List:
- ✓ closed under binary operation
- ✓ associativity
- ✓ Identity element
- ✓ Inverse

Have you thought of examples of groups you might know?



Real Numbers

- The real numbers $\mathbb{R}$ form a group, with respect to addition.

Check List:
- ✓ closed under binary operation
- ✓ associativity
- ✓ Identity element
- ✓ Inverse

Be Rational!
Get Real!
i
π

- What about multiplication?
- The real numbers without the zero form a group for multiplication.
- What about the set of complex numbers? (left as exercise)

Consider the set of integers $\mathbb{Z}$.

Definition 10. We say that $a, b \in \mathbb{Z}$ are congruent modulo n if their difference is an integer multiple of n. We write

$$a \equiv b \bmod n \Leftrightarrow a - b = t \cdot n, \quad t \in \mathbb{Z}.$$

Example 3. Here are a few examples of computation.

- $7 \equiv 2 \bmod 5$ because $7 - 2 = 1 \cdot 5$,
- $-6 \equiv -1 \bmod 5$ because $-6 - (-1) = (-1) \cdot 5$,
- $-1 \equiv 4 \bmod 5$ because $-1 - 4 = (-1) \cdot 5$,
- $-6 \equiv 4 \bmod 5$ because $4 - (-6) = 2 \cdot 5$.

We are of course interested in finding a group structure on integers mod n. To do so, we first need to recall what are equivalence classes.

Proposition 3. *Congruence mod n is an* ***equivalence relation*** *over the integers, i.e., it is a relation that is reflexive, symmetric and transitive.*

Proof. We need to verify that congruence mod n is indeed reflexive, symmetric, and transitive as claimed.

Reflexive: it is true that $a \equiv a \bmod n$ since $a - a = 0 \cdot n$.

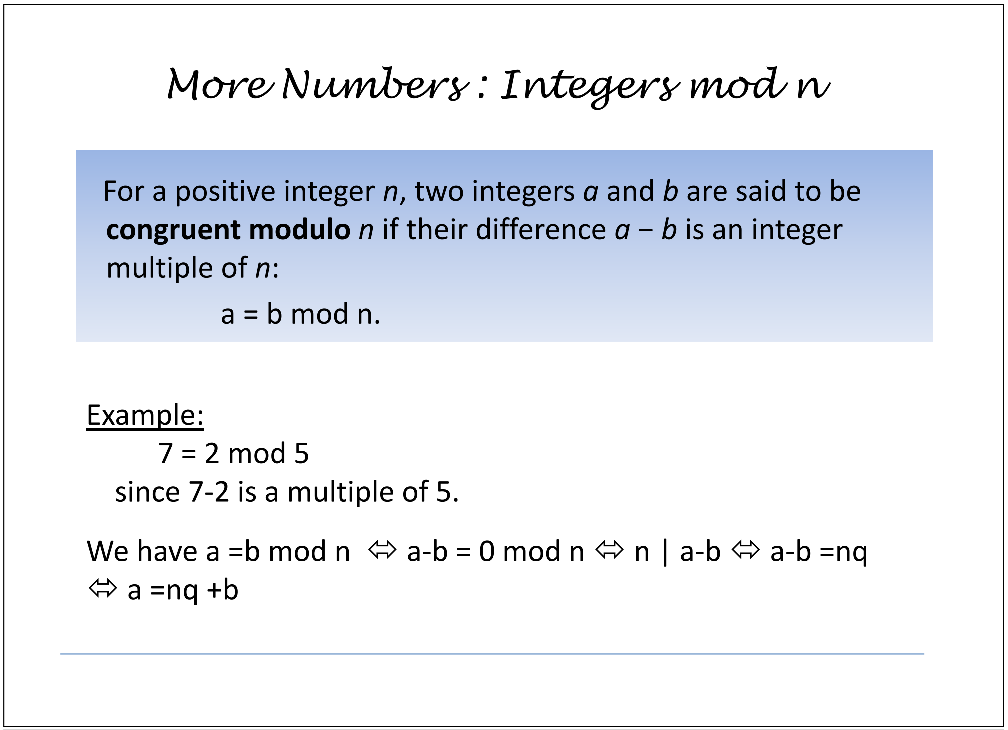
Symmetric: we show that if $a \equiv b \mod n$ then $b \equiv a \mod n$. Now $a \equiv b \mod n \iff a - b = tn \iff b - a = (-t)n \iff b \equiv a \mod n$.

Transitive: we show that if $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$. Now if $a - b = t_1 n$ and $b - c = t_2 n$, then $a - c = a - b + b - c = (t_1 + t_2)n$, showing that $a \equiv c \mod n$. ☐

Given an equivalence relation over a set, this relation always partitions it into equivalence classes. In particular, we get here:

Theorem 4. *Congruence* mod n *partitions the integers $\mathbb{Z}$ into (disjoint)* ***equivalence classes****, where the equivalence class of $a \in \mathbb{Z}$ is given by*

$$\bar{a} = \{b \in \mathbb{Z},\ a \equiv b \mod n\}.$$



More Numbers : Integers mod n

For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n* if their difference *a* − *b* is an integer multiple of *n*:

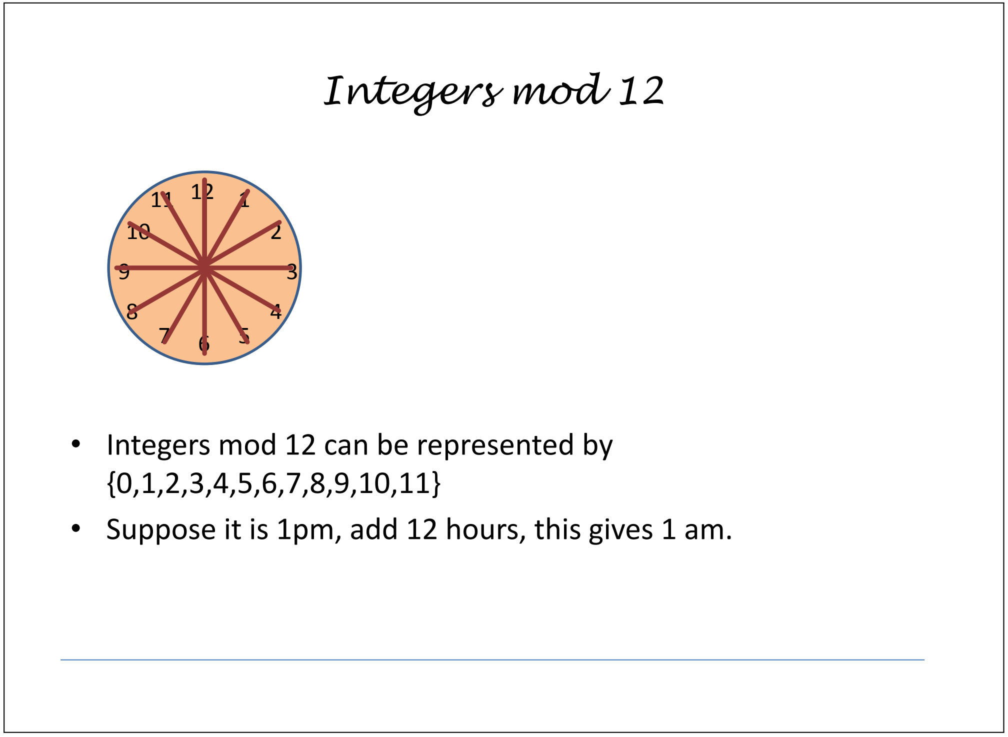
a = b mod n.

Example:

7 = 2 mod 5

since 7-2 is a multiple of 5.

We have a =b mod n ⇔ a-b = 0 mod n ⇔ n | a-b ⇔ a-b =nq ⇔ a =nq +b



Integers mod 12

12
1
2
3
4
5
6
7
8
9
10
11

- Integers mod 12 can be represented by {0,1,2,3,4,5,6,7,8,9,10,11}
- Suppose it is 1pm, add 12 hours, this gives 1 am.

Proof. Recall first that a "partition" refers to a disjoint union, thus we have to show that

$$\mathbb{Z} = \bigcup_{a\in\mathbb{Z}} \bar{a} = \bigcup_{a\in\mathbb{Z}} \{b \in \mathbb{Z},\ a \equiv b \mod n\}$$

where $\bar{a} \cap \bar{a'}$ is empty if $\bar{a} \neq \bar{a'}$. Since a runs through $\mathbb{Z}$, we already know that $\mathbb{Z} = \bigcup_{a\in\mathbb{Z}} \bar{a}$, thus the real work is to show that two equivalence classes are either the same or disjoint. Take

$$\bar{a} = \{b \in \mathbb{Z},\ a \equiv b \mod n\},\ \bar{a'} = \{b' \in \mathbb{Z},\ a' \equiv b' \mod n\}.$$

If the intersection $\bar{a} \cap \bar{a'}$ is empty, the two sets are disjoint. Let us thus assume that there is one element c which belongs to the intersection. Then

$$c \equiv a \mod n \text{ and } c \equiv a' \mod n \Rightarrow c = a + tn = a' + sn$$

for some integers s, t. But this shows that

$$a - a' = sn - tn = (s - t)n \Rightarrow a \equiv a' \mod n$$

and we concluce that the two equivalence classes are the same. □

Note that $a \equiv b \bmod n \iff a - b = t \cdot n \iff a = b + tn$, which means that both a and b have the same remainder when we divide them by n. Furthermore, since every integer $a \in \mathbb{Z}$ can be uniquely represented as $a = tn + r$ with $r \in \{0, 1, 2, \ldots, (n-1)\}$, we may choose r as the **representative** of a in its equivalence class under congruence mod n, which simply means that integers mod n will be written $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

Let us define now addition of integers mod n:

$$(a \mod n) + (b \mod n) \equiv (a + b) \mod n.$$

When we write $a \mod n$, we are chosing a as a representative of the equivalence class $\bar{a}$, and since the result of the addition involves a, we need to make sure that it will not change if we pick a' as a representative instead of a!

Proposition 4. *Suppose that $a' \equiv a$ mod n, and $b' \equiv b$ mod n, then $(a'$ mod $n) \pm (b'$ mod $n) \equiv (a \pm b)$ mod n.*

Proof. Since $a' \equiv a$ mod n, and $b' \equiv b$ mod n, we have by definition that

$$a' = a + qn,\ b' = b + rn,\ q, r \in \mathbb{Z}$$

hence

$$a' \pm b' = (a + qn) \pm (b + rn) = (a \pm b) + n(q \pm r) \equiv a \pm b \mod n.$$

□

Equivalence Relation

Being congruent mod n is an equivalence relation.

- It is reflexive: a = a mod n
- It is symmetric: if a=b mod n, then b=a mod n.
- It is transitive: if a=b mod n and b=c mod n, then a=c mod n

Thus if a = b mod n, they are in the same equivalence class.
We work with a representative of an equivalence class, it does not matter which (typically between 0 and n-1).

What it means: we identify all elements which are “the same” as one element, an equivalent class!

Addition modulo n

Let us define addition mod n:

(a mod n) + (b mod n) = (a+b) mod n

Problem: given a and n, there are many a’ such that a = a’ mod n, in fact, all the a’ in the equivalence class of a.
Thus addition should work independently of the choice of a’, that is, independently of the choice of the representative!

Take a’ = a mod n, b’=b mod n, then it must be true that (a’ mod n) + (b’ mod n) = (a+b) mod n.
a’ =a mod n ⇔ a’ = a +qn for some q
b’ =b mod n ⇔ b’ = b+rn for some r
Thus (a+qn)+(b+rn) = (a+b) + n(q+r) = a+b mod n.

All this work was to be able to claim the following:

$$\boxed{\text{The integers mod } n \text{ together with addition form a group } G,}$$

where by integers mod n we mean the n equivalence classes

$$G = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\},$$

also denoted by $\mathbb{Z}/n\mathbb{Z}$, and by addition, the binary law

$$\overline{a} + \overline{b} = (a+b) \mod n.$$

We indeed fullfil the definition of a group:

- Closure: since $(a+b) \mod n \in G$.
- Associativity.
- The identity element is $\overline{0}$, since $\overline{a} + \overline{0} = a \mod n = \overline{a}$.
- The inverse of a is $\overline{n-a}$, since $\overline{a} + \overline{n-a} = n \mod n = \overline{0}$.

We further have that G is commutative. Indeed $\overline{a_1} + \overline{a_2} = \overline{a_2} + \overline{a_1}$ (by commutativity of regular addition!).

Therefore G is an abelian group of order n. The group G of integers mod n has in fact more properties.

Proposition 5. *The group G of integers mod n together with addition is cyclic.*

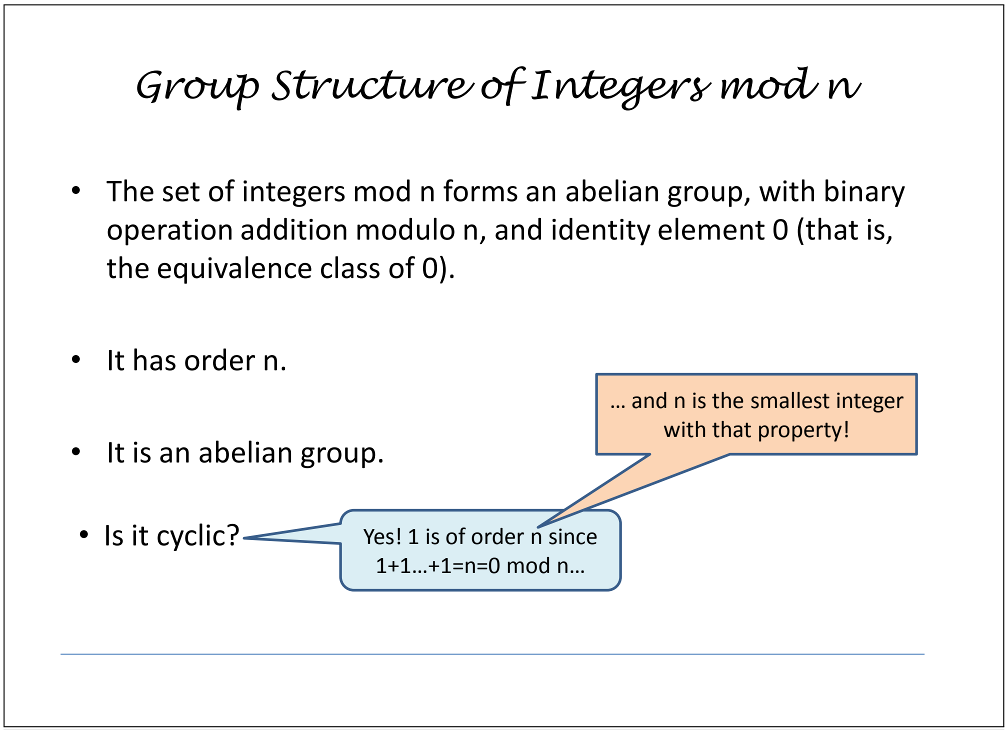
Proof. We have that G has order $|G| = n$. Recall that for a group to be cyclic, we need an element of G of order n, that is an element $\bar{a}$ such that (in additive notation)

$$\bar{a} + \dots \bar{a} = n\bar{a} = \bar{0}.$$

We take for $\bar{a}$ the element $\overline{1}$, which when repeatedly composed with itself will generate all the elements of the group as follows:

$$\begin{cases} \overline{1} + \overline{1} = \overline{2} \\ \overline{1} + \overline{1} + \overline{1} = \overline{3} \\ \vdots \\ \underbrace{\overline{1} + \overline{1} + \overline{1} + \dots + \overline{1}}_{(n-1) \ times} = \overline{n-1} \\ \underbrace{\overline{1} + \overline{1} + \overline{1} + \dots + \overline{1}}_{n \ times} = \overline{n} = \overline{0}. \end{cases}$$

□

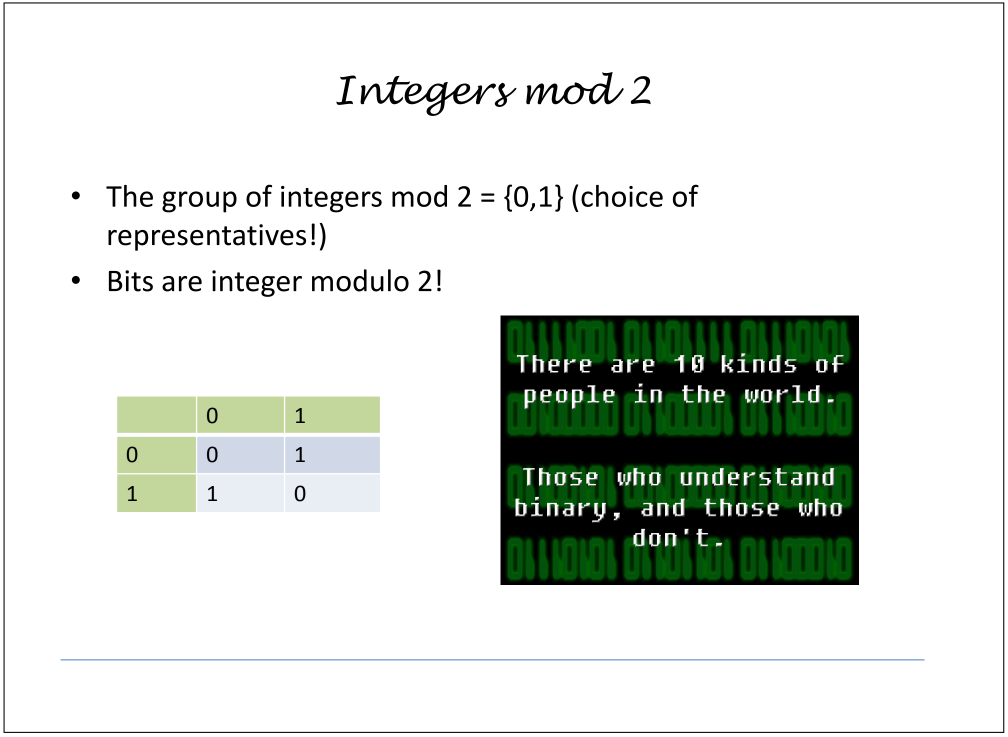


Group Structure of Integers mod n

- The set of integers mod n forms an abelian group, with binary operation addition modulo n, and identity element 0 (that is, the equivalence class of 0).
- It has order n.
- It is an abelian group.
- Is it cyclic?

Yes! 1 is of order n since 1+1…+1=n=0 mod n…

… and n is the smallest integer with that property!



Integers mod 2

- The group of integers mod 2 = {0,1} (choice of representatives!)
- Bits are integer modulo 2!

	0	1
0	0	1
1	1	0

There are 10 kinds of people in the world.

Those who understand binary, and those who don't.

Example 4. The group $(\mathbb{Z}/2\mathbb{Z}, +)$ of integers mod 2 has Cayley table

	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

and forms a cyclic group of order 2 ($\mathbb{Z}/2\mathbb{Z} = \langle\overline{1}\rangle$, $\overline{1}^2 = \overline{1} + \overline{1} = \overline{0}$).

Example 5. The group $(\mathbb{Z}/3\mathbb{Z}, +)$ of integers mod 3 has Cayley table

	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

This is a cyclic group of order 3: $\mathbb{Z}/3\mathbb{Z} = \langle\overline{1}\rangle = \langle\overline{2}\rangle$.

Example 6. The Cayley table of the group $(\mathbb{Z}/4\mathbb{Z}, +)$ of integers mod 4 is

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

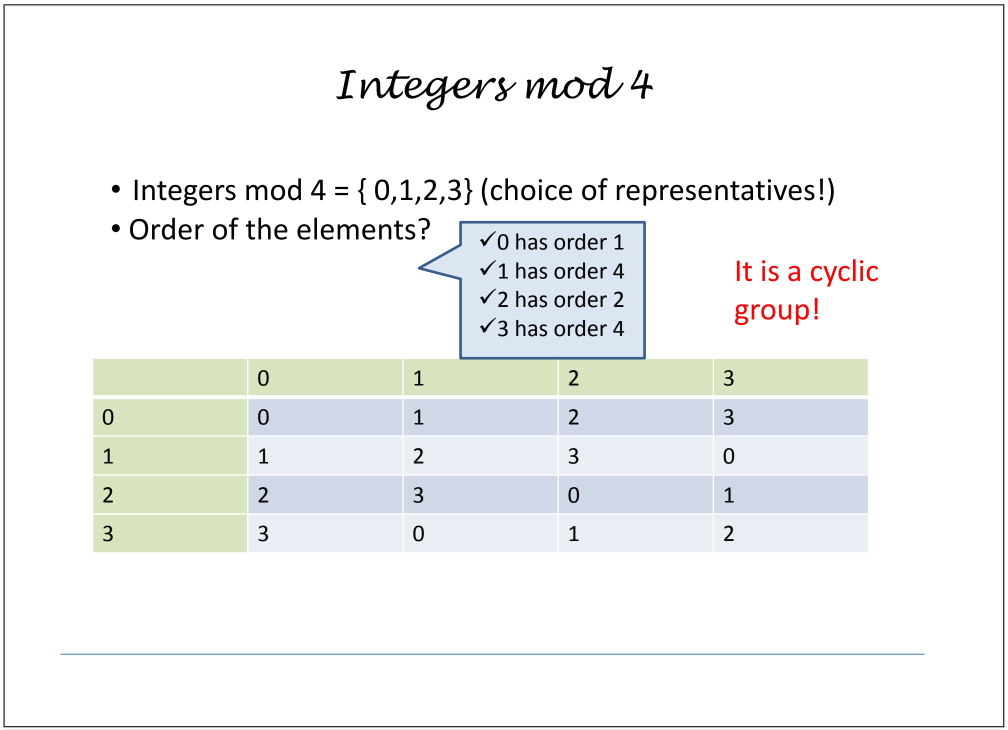
This is a cyclic group: $(\mathbb{Z}/4\mathbb{Z}, +) = \langle\overline{1}\rangle = \langle\overline{3}\rangle$. The subgroup $\langle\overline{2}\rangle = \{\overline{0}, \overline{2}\}$ of $(\mathbb{Z}/4\mathbb{Z}, +)$ has a Cayley table quite similar to that of $(\mathbb{Z}/2\mathbb{Z}, +)$!

	$\overline{0}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{0}$

A "historical" use of integers modulo n is credited to the Roman emperor Julius Caesar (100 BC 44 BC), who apparently was communicating with his army generals using what is now called *Caesar's cipher*. A modern way of explaining his cipher is to present it as an encryption scheme e_K defined by

$$e_K(x) = x + K \mod 26,\ K = 3$$

where x is an integer between 0 and 25, corresponding to a letter in the alphabet (for example, 0↦A,...,25↦Z). This is a valid encryption scheme, because it has a decryption function d_K such that $d_K(e_K(x)) = x$ for every integer x mod 26.



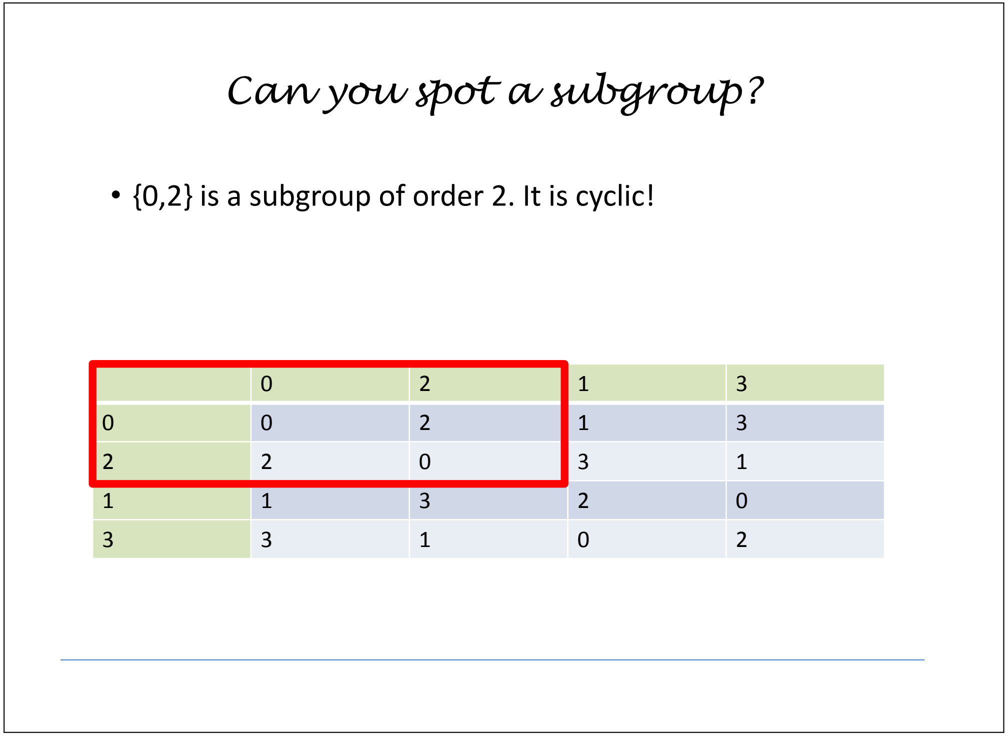
Integers mod 4

- Integers mod 4 = { 0,1,2,3} (choice of representatives!)
- Order of the elements?

✓0 has order 1
✓1 has order 4
✓2 has order 2
✓3 has order 4

It is a cyclic group!

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



Can you spot a subgroup?

- {0,2} is a subgroup of order 2. It is cyclic!

	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

After studying integers modulo n with respect to addition, we consider multiplication. First, we check that

$$(a \mod n) \cdot (b \mod n) \equiv (a \cdot b) \mod n$$

does not depend on the choice of a representative in $a \mod n$ and $b \mod n$.

Proposition 6. *Suppose that* $a' \equiv a \mod n$ *and* $b' \equiv b \mod n$*, then* $(a' \mod n) \cdot (b' \mod n) \equiv (a \cdot b) \mod n$*.*

Proof. We write $a' = a+qn$, $b' = b+rn$ and compute $a' \cdot b' = (a+qn)(b+rn) = ab + n(ar + qb + n)$ as needed! ☐

This operation obeys (1) closure, (2) associativity, and (3) there exists an identity element $\overline{1}$: $\overline{a} \cdot \overline{1} = \overline{a}$. But not every $\overline{a}$ has an inverse! For an inverse $\bar{a}^{-1}$ of $\bar{a}$ to exist, we need $aa^{-1} = 1 + zn$, where $z \in \mathbb{Z}$.

Example 7. If $n = 4$, 2 cannot have an inverse, because 2 multiplied by any integer is even, and thus cannot be equal to $1 + 4z$ which is odd.

To understand when an inverse exists, we will need the *Bézout's Identity.*

Theorem 5. *Let* a, b *be integers, with greatest common divisor* $\gcd(a, b) = d$*. Then there exist integers* m, n *such that*

$$am + bn = d.$$

Conversely, if $am' + bn' = d'$ *for some integers* m', n'*, then* d *divides* d'*.*

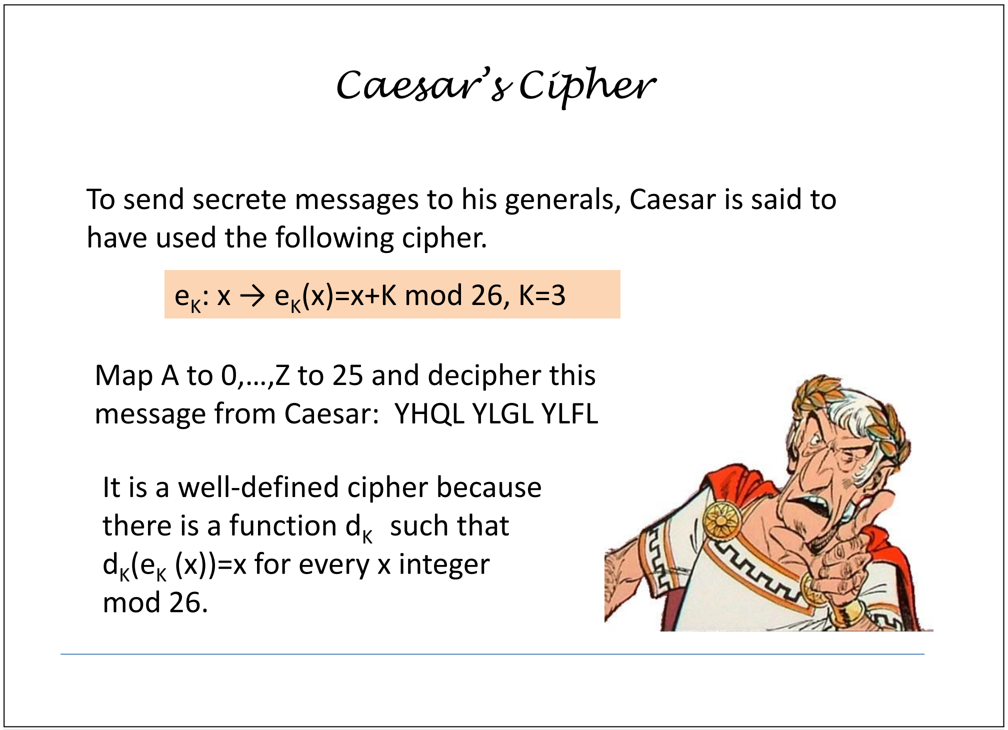
Proof. Recall that the Euclidean Algorithm computes $\gcd(a, b)$! Suppose $b < a$. Then we divide a by b giving a quotient q_0 and remainder r_0:

$$a = bq_0 + r_0,\ r_0 < b. \tag{4.1}$$

Next we divide b by r_0: $b = r_0 q_1 + r_1$, $r_1 < r_0$, and r_0 by r_1: $r_0 = r_1 q_2 + r_2$, $r_2 < r_1$ and we see the pattern: since $r_{k+1} < r_k$, we divide r_k by r_{k+1}

$$r_k = r_{k+1} q_{k+2} + r_{k+2},\ r_{k+2} < r_{k+1}. \tag{4.2}$$

Each step gives us a new nonnegative remainder, which is smaller than the previous one. At some point we will get a zero remainder: $r_N = r_{N+1} q_{N+2} + 0$.



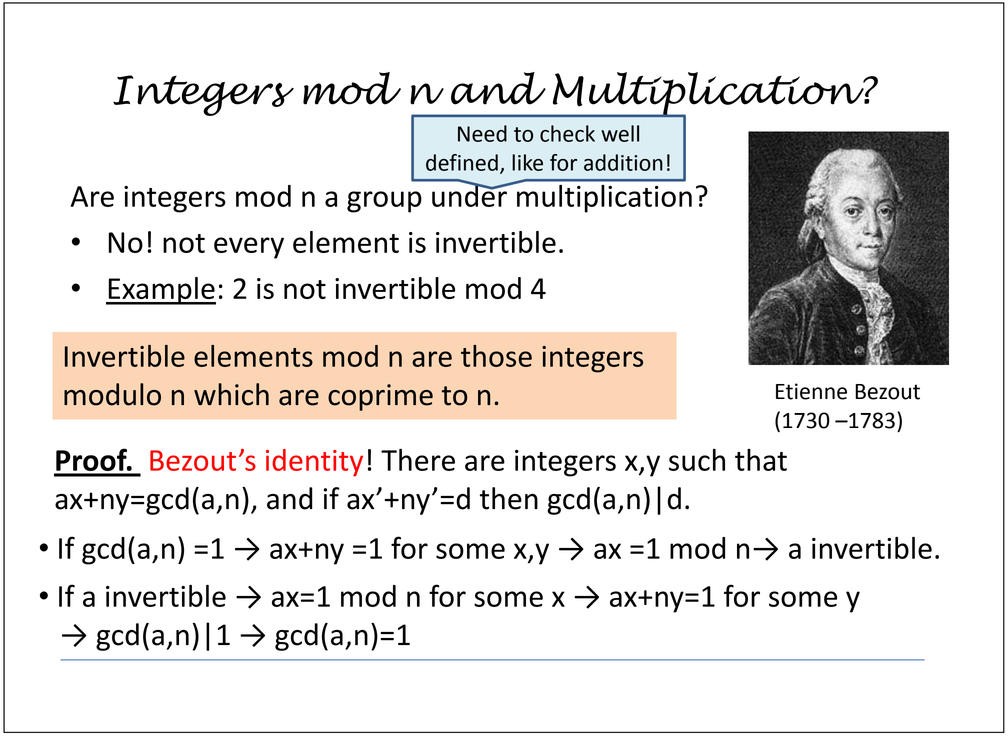
Caesar’s Cipher

To send secrete messages to his generals, Caesar is said to have used the following cipher.

$e_K: x \to e_K(x)=x+K \bmod 26, K=3$

Map A to 0,…,Z to 25 and decipher this message from Caesar: YHQL YLGL YLFL

It is a well-defined cipher because there is a function d_K such that $d_K(e_K(x))=x$ for every x integer mod 26.



Integers mod n and Multiplication?

Need to check well defined, like for addition!

Are integers mod n a group under multiplication?

- No! not every element is invertible.
- Example: 2 is not invertible mod 4

Invertible elements mod n are those integers modulo n which are coprime to n.

Etienne Bezout (1730 –1783)

Proof. Bezout’s identity! There are integers x,y such that ax+ny=gcd(a,n), and if ax’+ny’=d then gcd(a,n)|d.

- If gcd(a,n) =1 → ax+ny =1 for some x,y → ax =1 mod n→ a invertible.
- If a invertible → ax=1 mod n for some x → ax+ny=1 for some y → gcd(a,n)|1 → gcd(a,n)=1

We now show inductively that $d = \gcd(a,b)$ is equal to r_{N+1}. The line (4.1) shows that $\gcd(a,b)$ divides r_0. Hence $\gcd(a,b) \mid \gcd(b,r_0)$. Suppose that $\gcd(a,b) \mid \gcd(r_{N-1},r_N)$. Since $r_{N-1} = r_N q_{N+1} + r_{N+1}$, we have that $\gcd(r_{N-1},r_N)$ divides both r_{N+1} and r_N thus it divides $\gcd(r_{N+1},r_N)$. Thus $\gcd(a,b) | \gcd(r_{N-1},r_N) | \gcd(r_N,r_{N+1}) = r_{N+1}$. On the other hand, backtracking, we see that r_{N+1} divides a,b: $r_{N+1} \mid r_N$ thus since $r_{N-1} = r_N q_{N+1} + r_{N+1}$, we have $r_{N+1} \mid r_{N-1}, \ldots$

To show Bézout's identity, we write $d = r_{N+1} = r_{N-1} - r_N q_{N+1}$, and substitute for each remainder its expression in terms of the previous remainders

$$r_{k+2} = r_k - r_{k+1} q_{k+2}$$

all the way back until the only terms involved are a, b. This gives that $d = r_{N+1} = am + bn$ for some $m, n \in \mathbb{Z}$, as desired.

Conversely, let d' be a positive integer. Suppose that $am' + bn' = d'$ for some integers m', n'. By definition of greatest common divisor, d divides a and b. Thus there exist integers a', b' with $a = da'$ and $b = db'$, and

$$da'm' + db'n' = d'.$$

Now d divides the two terms of the sum, thus it divides d'. □

We are ready to characterize integers mod n with a multiplicative inverse.

Corollary 1. *The integers mod n which have multiplicative inverses are those which are coprime to n, i.e. , $\{\bar{a}, \mid \gcd(a,n) = 1\}$.*

Proof. If $\gcd(a,n) = 1$, Bézout's identity tells us that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Thus $ax = 1 + (-y)n$ and $\overline{x}$ is the inverse of a.

Conversely, if there is an $\overline{x}$ such that $\overline{ax} = \overline{1}$ then $ax = 1 + yn \iff ax - yn = 1$ for some $y \in \mathbb{Z}$. By Bézout's identity, we have $\gcd(a,n) \mid 1$, showing that $\gcd(a,n) = 1$. □

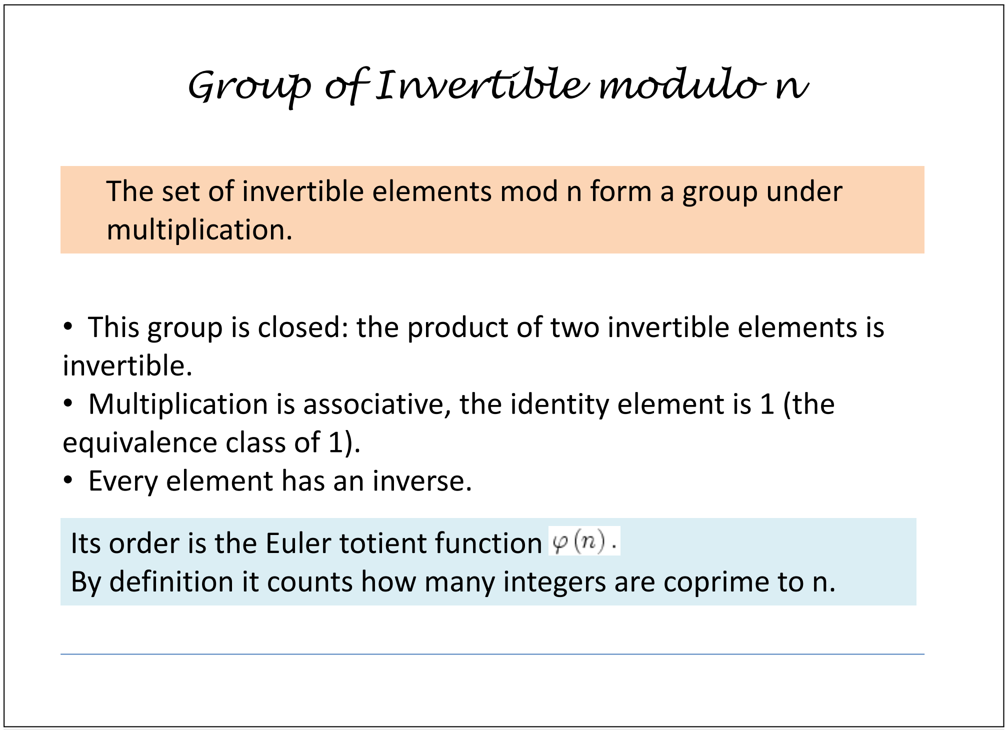
The set $(\mathbb{Z}/n\mathbb{Z})^*$ of invertible elements mod n forms a group under multiplication.

Indeed (a) closure holds: $(\overline{a}\overline{b})^{-1} = (\overline{b}^{-1})(\overline{a}^{-1}) \in (\mathbb{Z}/n\mathbb{Z})^*$, (b) associativity holds, (c) the identity element is $\overline{1}$, (d) every element is invertible (we just proved it!).

What is the order of this group?

$$|(\mathbb{Z}/n\mathbb{Z})^*| = \#\{a \in \{0,1,2,\ldots,(n-1)\} \mid \gcd(a,n) = 1\} = \varphi(n),$$

where $\varphi(n)$ is a famous function called the Euler totient, which by definition counts the number of positive integers coprime to n.

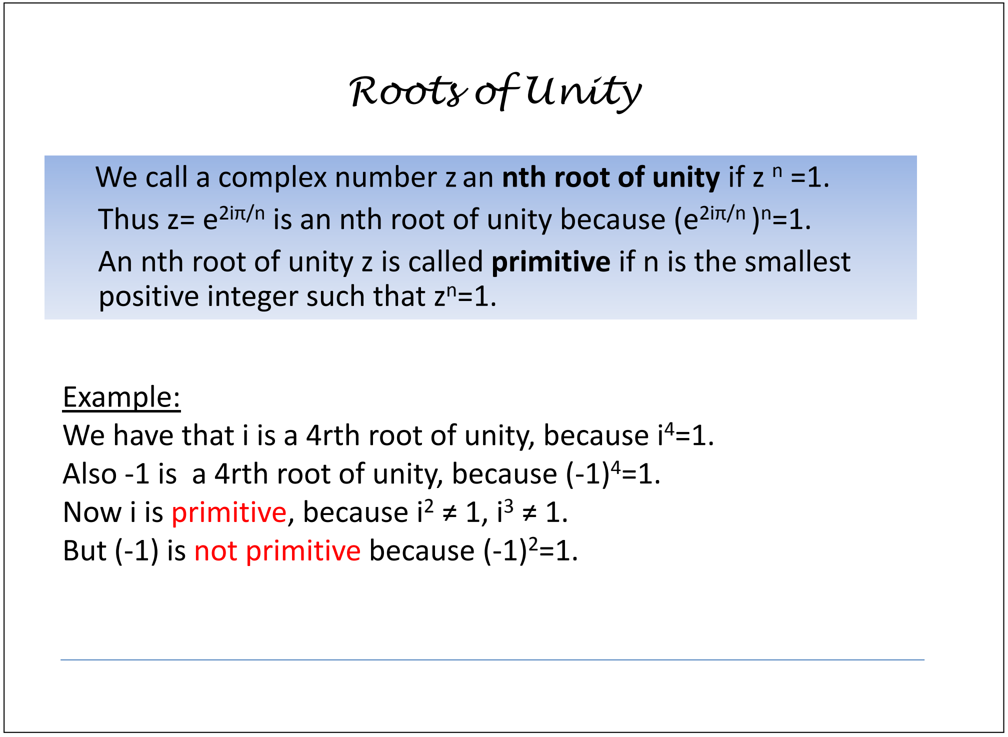


Group of Invertible modulo n

The set of invertible elements mod n form a group under multiplication.

- This group is closed: the product of two invertible elements is invertible.
- Multiplication is associative, the identity element is 1 (the equivalence class of 1).
- Every element has an inverse.

Its order is the Euler totient function $\varphi(n)$.
By definition it counts how many integers are coprime to n.



Roots of Unity

We call a complex number z an **nth root of unity** if $z^n=1$.
Thus $z=e^{2i\pi/n}$ is an nth root of unity because $(e^{2i\pi/n})^n=1$.
An nth root of unity z is called **primitive** if n is the smallest positive integer such that $z^n=1$.

Example:
We have that i is a 4rth root of unity, because $i^4=1$.
Also -1 is a 4rth root of unity, because $(-1)^4=1$.
Now i is primitive, because $i^2 \neq 1$, $i^3 \neq 1$.
But (-1) is not primitive because $(-1)^2=1$.

Let us see one more example of a group. From the complex numbers, a very special discrete set is that of nth roots of unity, which by definition is

$$\omega^{(n)} = \{w \in \mathbb{C} \mid w^n = 1\} = \{e^{i\frac{2\pi}{n}k},\ k = 1, 2, \dots, n\},$$

since $(e^{i\frac{2\pi}{n}k})^n = e^{i2\pi k} = 1$ for any $k \in \mathbb{Z}$. Note that the polynomial $X^n - 1 = 0$ has at most n roots, and we found already n of them, given by $e^{i\frac{2\pi}{n}k}$, $k = 1, \dots, n$, thus there is no another nth root of unity.

$$\boxed{\text{The set } \omega^{(n)} \text{ of } n\text{th roots of unity forms a group under multiplication.}}$$

Indeed, (a) closure is satistifed: $e^{i\frac{2\pi}{n}k_1}e^{i\frac{2\pi}{n}k_2} = e^{i\frac{2\pi}{n}(k_1+k_2)} \in \omega^{(n)}$, (b) as is associativity. (c) The identity element is 1. Finally (d) every element in $\omega^{(n)}$ is invertible: $(e^{i\frac{2\pi}{n}k_1})^{-1} = e^{i\frac{2\pi}{n}(-k_1)}$.

We also have commutativity since $e^{i\frac{2\pi}{n}k_1}e^{i\frac{2\pi}{n}k_2} = e^{i\frac{2\pi}{n}(k_1+k_2)} = e^{i\frac{2\pi}{n}k_2}e^{i\frac{2\pi}{n}k_1}$.

An nth root of unity ω is said to be primitive if n is the smallest positive integer for which $\omega^n = 1$. But then, since $\omega^{(n)}$ has n elements, all the nth roots of unity are obtained as a power of ω! For example, take $\omega = e^{i\frac{2\pi}{n}}$ (you may want to think of another example of primitive nth root of unity!), then

$$\{\omega^k = e^{i\frac{2\pi}{n}k},\ k = 1, \dots, n\} = \omega^{(n)}.$$

We just proved the following:

Proposition 7. *The group $(\omega^{(n)}, \cdot)$ of nth roots of unity is a cyclic group of order n generated by a primitive nth root of unity, e.g. $\omega = e^{i\frac{2\pi}{n}}$.*

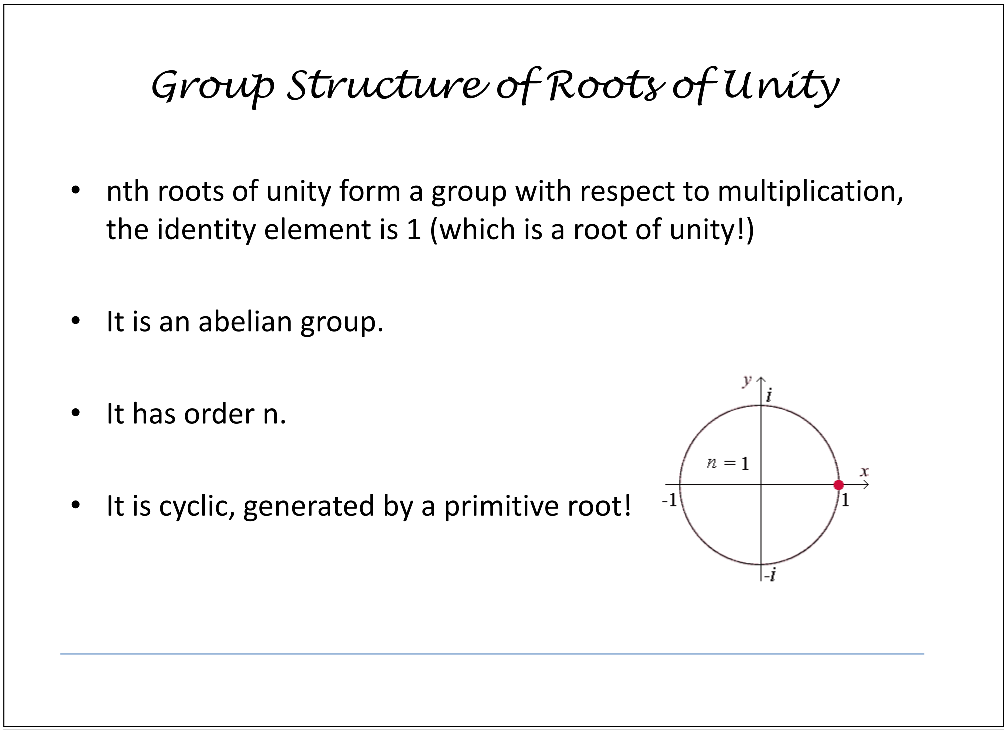
Example 8. Consider $(\omega^{(3)}, \cdot) = (\{1, e^{i\frac{2\pi}{3}}, e^{i\frac{2\pi}{3}2}\}, \cdot)$. There are two primitive roots of unity. Set $\omega = e^{i\frac{2\pi}{3}}$. The Cayley table of $(\omega^{(3)}, \cdot)$ is

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Example 9. Consider $(\omega^{(4)}, \cdot) = (\{1, i, -1, -i\}, \cdot)$, with Cayley table

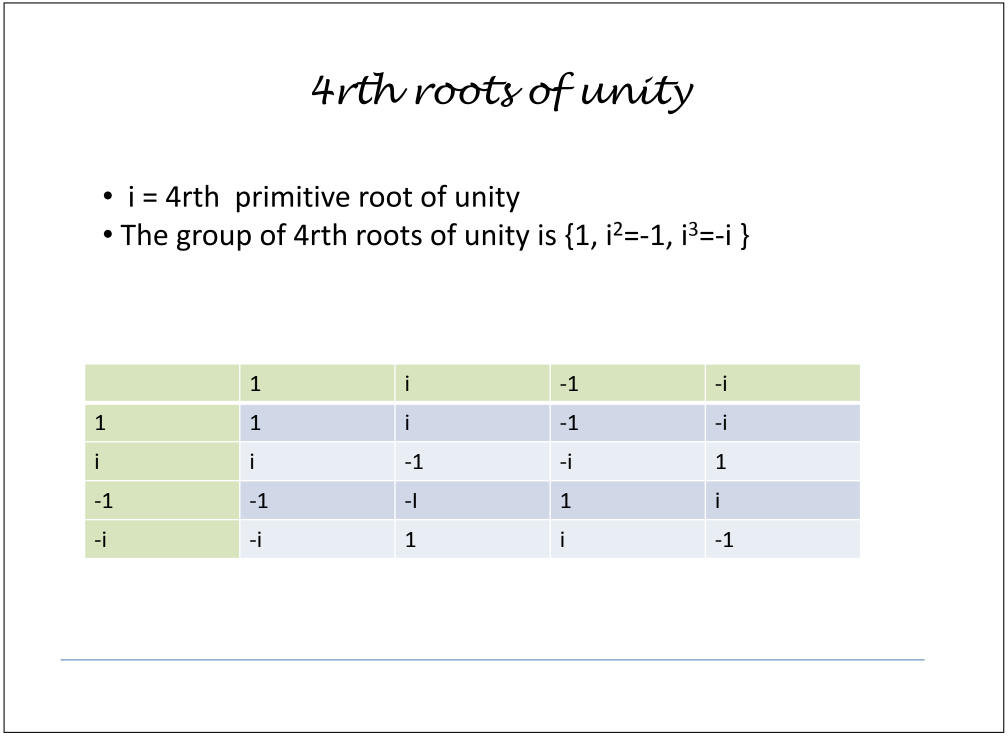
	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

So i is a primitive 4th root of unity since $i \neq 1, i^2 = -1, i^3 = -i, i^4 = 1$ and $\langle i \rangle = \omega^{(4)}$, but -1 is not a primitive root because $(-1)^2 = 1$.



Group Structure of Roots of Unity

- nth roots of unity form a group with respect to multiplication, the identity element is 1 (which is a root of unity!)
- It is an abelian group.
- It has order n.
- It is cyclic, generated by a primitive root!



4rth roots of unity

- i = 4rth primitive root of unity
- The group of 4rth roots of unity is {1, i^2=-1, i^3=-i }

	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-I	1	i
-i	-i	1	i	-1

So far we have seen many examples of groups: integers mod n with addition, invertible integers mod n with multiplication, nth roots of unity with multiplication, $\mathbb{R}$ with addition, $\mathbb{R}^*$ with multiplication, and all those groups we saw as symmetries (that of the square, of the rectangle, of triangles...) with composition. Among them, some were infinite, some were finite, some were cyclic, some not, some of the groups were abelian, some were not.

The time has come ("the Walrus said" ...) to sort things out a bit, and try to "quantify" the similarity or dissimilarity of the group structures we encountered in our "group zoo".

We start here to develop tools for analyzing and classifying group structure. Suppose we are given two groups $(G, \cdot)$ and $(H, *)$ with possibly different sets G, H and respective binary operation $\cdot$ and $*$.

Definition 11. A map $f : G \to H$ which obeys

$$\underbrace{f(\underbrace{g_l \cdot g_k}_{\text{in G}})}_{\text{in H}} = \underbrace{f(g_l) * f(g_k)}_{\text{in H}}, \text{ for all } g_k, g_l \in G$$

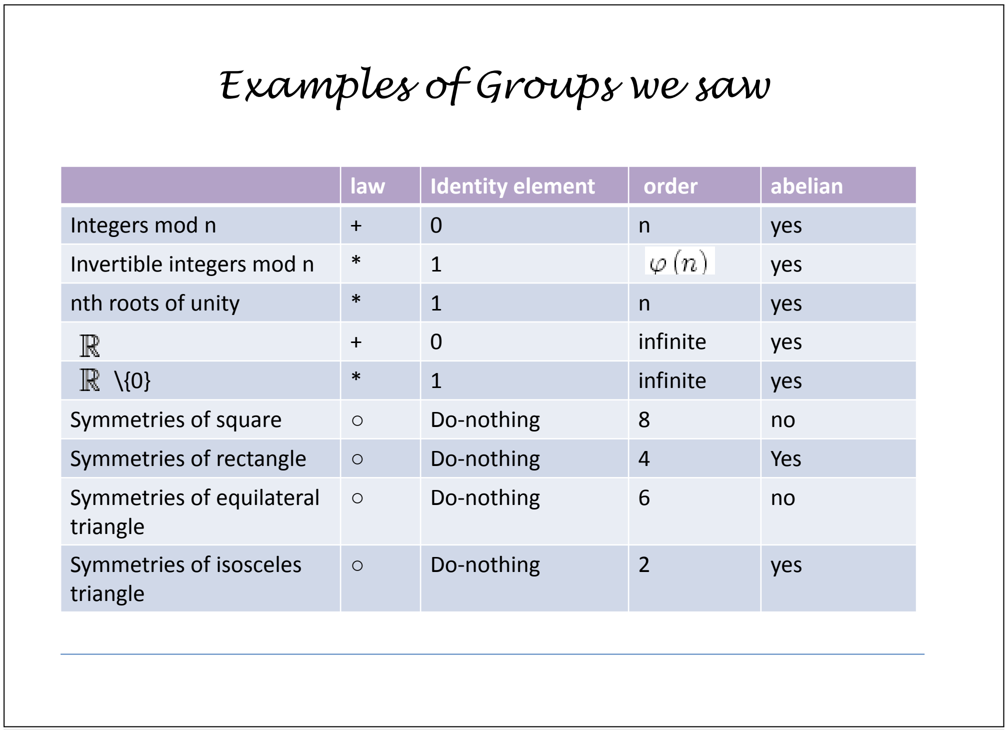
is called a group homomorphism.

Recall that a map $f : G \to H$ which takes elements of the set G and pairs them with elements of H is called

- injective or one-to-one, if no two different elements g_1, g_2 of G map to the same $h \in H$, i.e., $f(g_1) \neq f(g_2)$ if $g_1 \neq g_2$.
- surjective or onto if for all $h \in H$, there exists $g \in G$ so that $f(g) = h$.
- bijective if it is both injective and surjective.

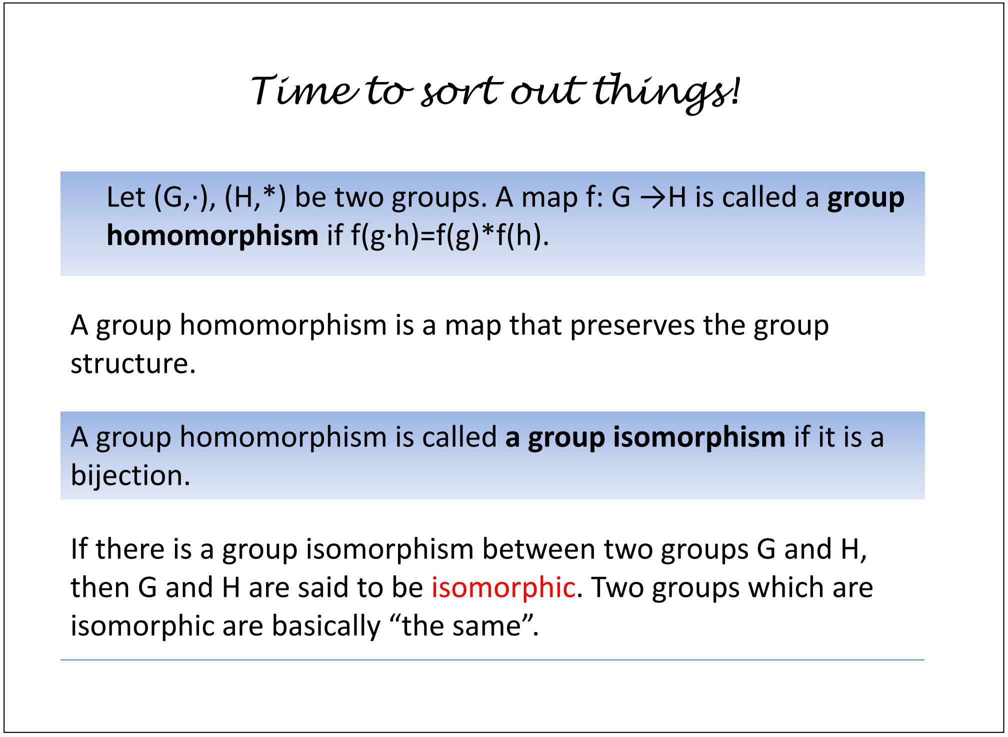
Definition 12. If $f : G \to H$ is a group homomorphism and also a bijection, then it is called a group isomorphism. We then say that G and H are isomorphic, written $G \simeq H$.

Maybe it will be easier to remember this word by knowing its origin: iso $\equiv$ same, morphis $\equiv$ form or shape. Let us see a first example of group homomorphism.



Examples of Groups we saw

	law	Identity element	order	abelian
Integers mod n	+	0	n	yes
Invertible integers mod n	*	1	$\varphi(n)$	yes
nth roots of unity	*	1	n	yes
$\mathbb{R}$	+	0	infinite	yes
$\mathbb{R}$ \{0}	*	1	infinite	yes
Symmetries of square	○	Do-nothing	8	no
Symmetries of rectangle	○	Do-nothing	4	Yes
Symmetries of equilateral triangle	○	Do-nothing	6	no
Symmetries of isosceles triangle	○	Do-nothing	2	yes



Time to sort out things!

Let (G,·), (H,*) be two groups. A map f: G →H is called a **group homomorphism** if f(g·h)=f(g)*f(h).

A group homomorphism is a map that preserves the group structure.

A group homomorphism is called **a group isomorphism** if it is a bijection.

If there is a group isomorphism between two groups G and H, then G and H are said to be isomorphic. Two groups which are isomorphic are basically “the same”.

Example 10. Consider the group $(\mathbb{Z}/4\mathbb{Z},+)$ of integers mod 4, as in Example 6, with Cayley table

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

and the group $(\omega^{(4)},\cdot)$ of 4rth roots of unity whose Cayley table

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

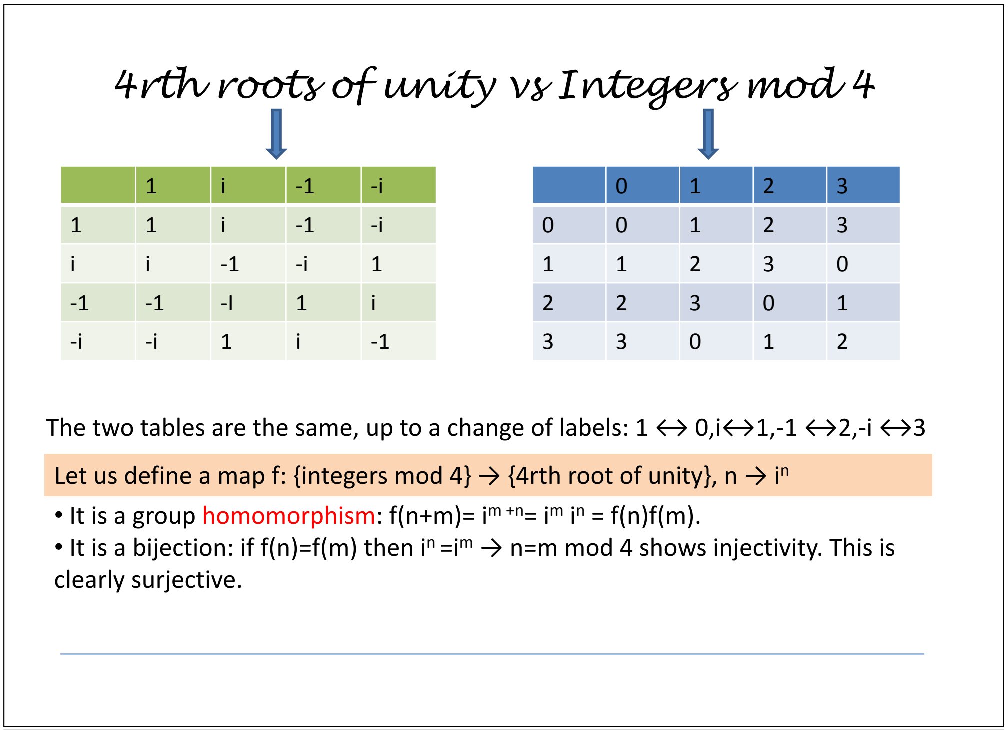
was computed in Example 9. These two groups are isomorphic, which can be seen on the Cayley tables, because they are the same, up to a change of labels ($1 \leftrightarrow 0$,$i \leftrightarrow 1$,$-1 \leftrightarrow 2$,$-i \leftrightarrow 3$). Formally, we define a map

$$f:(\mathbb{Z}/4\mathbb{Z},+)\to(\omega^{(4)},\cdot),\ m\mapsto i^m.$$

Firstly, we need to check that it is well defined, that is, if we choose $m' \equiv m \mod 4$, then $f(m') = f(m)$:

$$f(m') = f(m+4r) = i^{m+4r} = i^m,\ r\in\mathbb{Z}.$$

It is a group homomorphism, since $f(n+m) = i^{m+n} = i^n i^m = f(n)f(m)$. It is also a bijection: if $f(n) = f(m)$, then $i^n = i^m$ and $n \equiv m \mod 4$, which shows injectivity. The surjectivity is clear (check that every element has a preimage, there are 4 of them to check!)



4rth roots of unity vs Integers mod 4

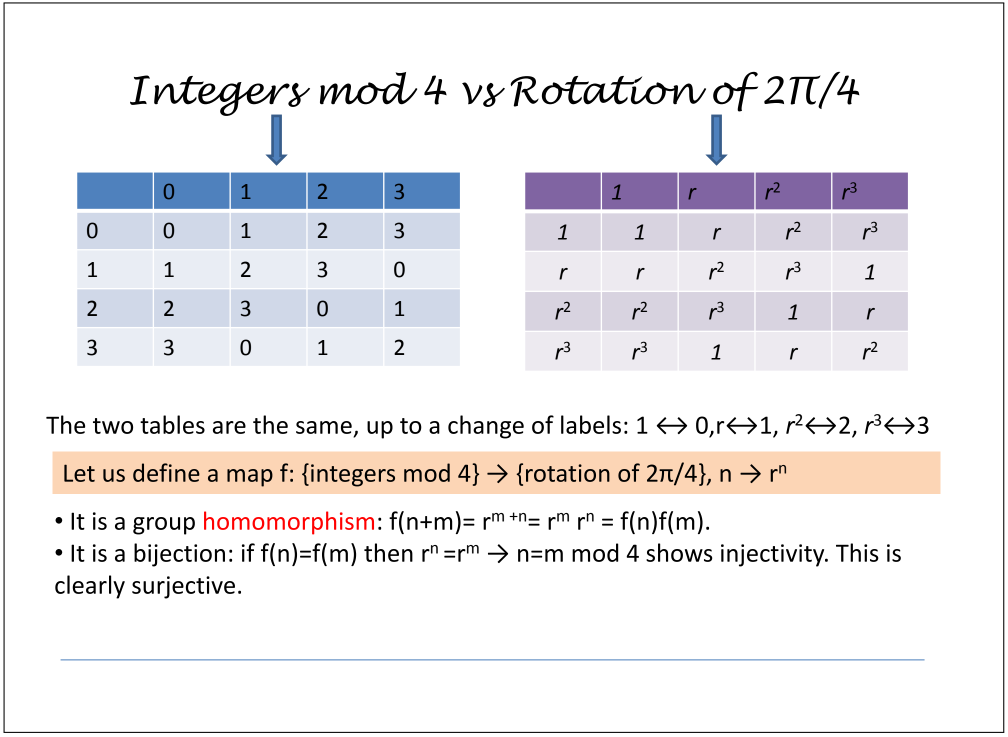
	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-I	1	i
-i	-i	1	i	-1

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The two tables are the same, up to a change of labels: 1 ↔ 0,i↔1,-1 ↔2,-i ↔3

Let us define a map f: {integers mod 4} → {4rth root of unity}, n → i^n

- It is a group homomorphism: f(n+m)= i^{m+n}= $i^m i^n$ = f(n)f(m).
- It is a bijection: if f(n)=f(m) then $i^n = i^m$ → n=m mod 4 shows injectivity. This is clearly surjective.



Integers mod 4 vs Rotation of 2π/4

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

	1	r	r^2	r^3
1	1	r	r^2	r^3
r	r	r^2	r^3	1
r^2	r^2	r^3	1	r
r^3	r^3	1	r	r^2

The two tables are the same, up to a change of labels: 1 ↔ 0,r↔1, r^2↔2, r^3↔3

Let us define a map f: {integers mod 4} → {rotation of 2π/4}, n → r^n

- It is a group homomorphism: f(n+m)= r^{m+n}= $r^m r^n$ = f(n)f(m).
- It is a bijection: if f(n)=f(m) then $r^n = r^m$ → n=m mod 4 shows injectivity. This is clearly surjective.

Example 11. Similarly, we can show that the group $(\mathbb{Z}/4\mathbb{Z}, +)$ is isomorphic to the group of rotations by an angle of $2\pi/4$, whose Cayley table is

	1	r	r^2	r^3
1	1	r	r^2	r^3
r	r	r^2	r^3	1
r^2	r^2	r^3	1	r
r^3	r^3	1	r	r^2

by considering the map

$$f : (\mathbb{Z}/4\mathbb{Z}, +) \to (\text{rotations of the square}, \circ),\ n \mapsto r^n.$$

It is well-defined (as in the above example) and is a group homomorphism, since $f(n+m) = r^{m+n} = r^n r^m = f(n)f(m)$. It is also a bijection: if $f(n) = f(m)$, then $r^n = r^m$ and $n \equiv m \mod 4$, which shows injectivity. The surjectivity is clear as above.

Let us summarize briefly what happened in this chapter. In the first half, we showed that we already know in fact more groups than we thought! The list includes the integers modulo n with addition, the invertible integers modulo n with multiplication, the roots of unity, etc

We then decided to start to classify a bit all these groups, thanks to the notion of group isomorphism, a formal way to decide when two groups are essentially the same! We then showed that integers mod 4, 4rth roots of unity, and rotations of the square are all isomorphic! We will see more of group classification in the coming chapters!

Exercises for Chapter 4

Exercise 21. We consider the set $\mathbb{C}$ of complex numbers.

1. Is $\mathbb{C}$ a group with respect to addition?
2. Is $\mathbb{C}$ a group with respect to multiplication?
3. In the case where $\mathbb{C}$ is a group, what is its order?
4. Can you spot some of its subgroups?

Exercise 22. Alice and Bob have decided to use Caesar's cipher, however they think it is too easy to break. Thus they propose to use an affine cipher instead, that is

$$e_K(x) = k_1 x + k_2 \mod 26, \;\; K = (k_1, k_2).$$

Alice chooses $K = (7, 13)$, while Bob opts for $K = (13, 7)$. Which cipher do you think will be the best? Or are they both equally good?

Exercise 23. Show that the map $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot),\; x \mapsto \exp(x)$ is a group homomorphism.

Exercise 24. Show that a group homomorphism between two groups G and H always maps the identity element 1_G to the identity element 1_H.

Exercise 25. In this exercise, we study a bit the invertible integers modulo n.

1. Take $n = 5$, and compute the group of invertible integers modulo 5. What is the order of this group? Can you recognize it? (in other words, is this group isomorphic to one of the groups we have already classified?)
2. Take $n = 8$, and compute the group of invertible integers modulo 8. What is the order of this group? Can you recognize it? (in other words, is this group isomorphic to one of the

   groups we have already classified?)

Exercise 26. Let f be a group homomorphism $f : G \to H$ where G and H are two groups. Show that

$$f(g^{-1}) = f(g)^{-1}.$$

Exercise 27. Consider the group $(\mathbb{Z}, +)$ of integers under addition. Let H be a subgroup of $\mathbb{Z}$.

1. Show that H is of infinite order.
2. Use the Euclidean division algorithm to show that H is generated by a single element.
3. Find a subset of $\mathbb{Z}$ which forms a multiplicative group.

Here is a guided version of this exercise. Please try to do the normal version first!

1. Recall first what the order of a group is, to understand what it means for H to be of infinite order. Once this is clear, you need to use one of the properties of a group! If you cannot see which one, try each of them (can you cite the 4 of them?) and see which one will help you!
2. This one is more difficult. You will need to use a trick, namely use the minimality of some element...In every subgroup of $\mathbb{Z}$, there is a smallest positive integer (pay attention to the word"subgroup" here, this does not hold for a subset!).
3. To have a multiplicative group (that is a group with respect to multiplication), you need to define a set, and make sure this set together with multiplication satisfies the usual 4 properties of a group!

Exercise 28. When we define a map on equivalence classes, the first thing we must check is that the map is *well defined*, that is, the map is independent of the choice of the representative of the equivalence class. In this exercise we give an example of a map which is *not well defined*.

Recall the parity map $sgn : \mathbb{Z} \to \mathbb{Z}/2$

$$sgn(2k+1) \mapsto 1$$

$$sgn(2k) \mapsto 0$$

Let $\mathbb{Z}/5\mathbb{Z}$ be the group of integers modulo 5. Let us attempt to define the map $sgn : \bar{a} \mapsto \overline{sgn(a)}$. Show that sgn is not well-defined on $\mathbb{Z}/5\mathbb{Z}$.

Chapter 5

More Group Structures

> *"The theory of groups is a branch of mathematics in which one does something to something and then compares the results with the result of doing the same thing to something else, or something else to the same thing. Group theory lets you see the similarities between different things, or the ways in which things can't be different, by expressing the fundamental symmetries."(J. Newman, Mathematics and the Imagination.)*

In the 4 previous chapters, we saw many examples of groups, coming from planar isometries and from numbers. In Chapter 4, we started to classify a bit some of our examples, using the notion of group isomorphism. The goal of this chapter is to continue this classification in a more systematic way!

What happened in Examples 10 and 11 is that the three groups considered (the integers mod 4, the 4rth roots of unity, and the rotations of the square) are all cyclic of order 4. As we shall see next, all cyclic groups of a given order are in fact isomorphic. Hence, from a structural point they are the same. We shall call the equivalent (up to isomorphism) cyclic group of order n, or the infinite cyclic group, as respectively

the cyclic group C_n of order n if $n < \infty$, or the infinite cyclic group C_∞ otherwise.

Theorem 6. *Any infinite cyclic group is isomorphic to the additive group of integers* $(\mathbb{Z}, +)$. *Any cyclic group of order* n *is isomorphic to the additive group* $(\mathbb{Z}/n\mathbb{Z}, +)$ *of integers mod* n.

Before starting the proof, let us recall that $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Its order is $|\mathbb{Z}| = \infty$.

The Cyclic Group C_n

- We just saw 3 cyclic groups of order 4, all of them with same multiplication table. They are essentially the "same group", thus to analyze them, there is no need to distinguish them.

Theorem. An infinite cyclic group is isomorphic to the additive group of integers, while a cyclic group of order *n* is isomorphic to the additive group of integers modulo n.

This is also saying that there is exactly one cyclic group (up to isomorphism) whose order is *n*, denoted by C_n and there is exactly one infinite cyclic group.

Proof of Theorem

A cyclic group is generated by one element (multiplicative notation)

Part 1

- Let G be an infinite cyclic group, G=<x>, g of order infinite. Define the map f:{group of integers}→G, $f(n)=x^n$.
- This is a group homorphism: $f(m+n)= x^{n+m} = x^n x^m=f(m)f(n)$.
- This is a bijection, thus we have a group isomorphism.

Part 2

- Let G be a cyclic group of order n, G=<x>, with g of order n. Define the map f:{group of integers mod n}→G, $f(n)= x^n$.
- This is a group homorphism: $f(m+n)= x^{n+m} = x^n x^m=f(m)f(n)$.
- This is a bijection, thus we have a group isomorphism.

Proof. Let G be a cyclic group. Whether it is finite or not, a cyclic group is generated by one of its elements g, i.e., $\langle g\rangle = G$. Define the map

$$\begin{cases} f : \mathbb{Z} \to G, & k \mapsto f(k) = g^k \quad \text{if } |G| = \infty \\ f : \mathbb{Z}/n\mathbb{Z} \to G, & k \mapsto f(k) = g^k \quad \text{if } |G| = n < \infty. \end{cases}$$

Note that $f : \mathbb{Z}/n\mathbb{Z} \to G$ is *well-defined*, since it does not depend on the choice of k as a representative of the equivalence class of $k \mod n$. Indeed, if $k' \equiv k \mod n$, then $k' = k + sn$ for some integer s, and

$$f(k') = f(k + sn) = g^{k+sn} = g^k g^{sn} = g^k.$$

This map is bijective (one-to-one and onto) and

$$f(k + l) = g^{k+l} = g^k \cdot g^l = f(k) \cdot f(l),$$

hence it is a homomorphism that is bijective. It is then concluded that f is an isomorphism between the integers and any cyclic group. □

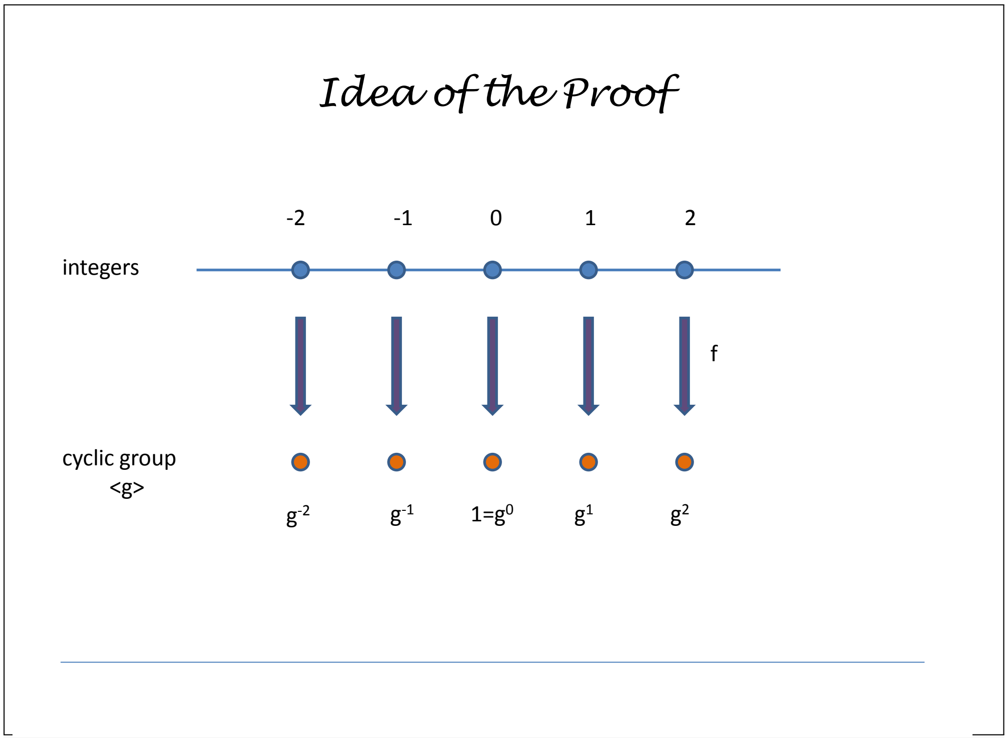
Example 12. With this theorem, to prove that the integers mod 4, the 4rth roots of unity, and the rotations of the square are isomorphic, it is enough to know that are all cyclic of order 4. Thus

$$C_4 \simeq (\mathbb{Z}/4\mathbb{Z}, +) \simeq (\omega^{(4)}, \cdot) \simeq (\text{rotations of the square}, \circ).$$

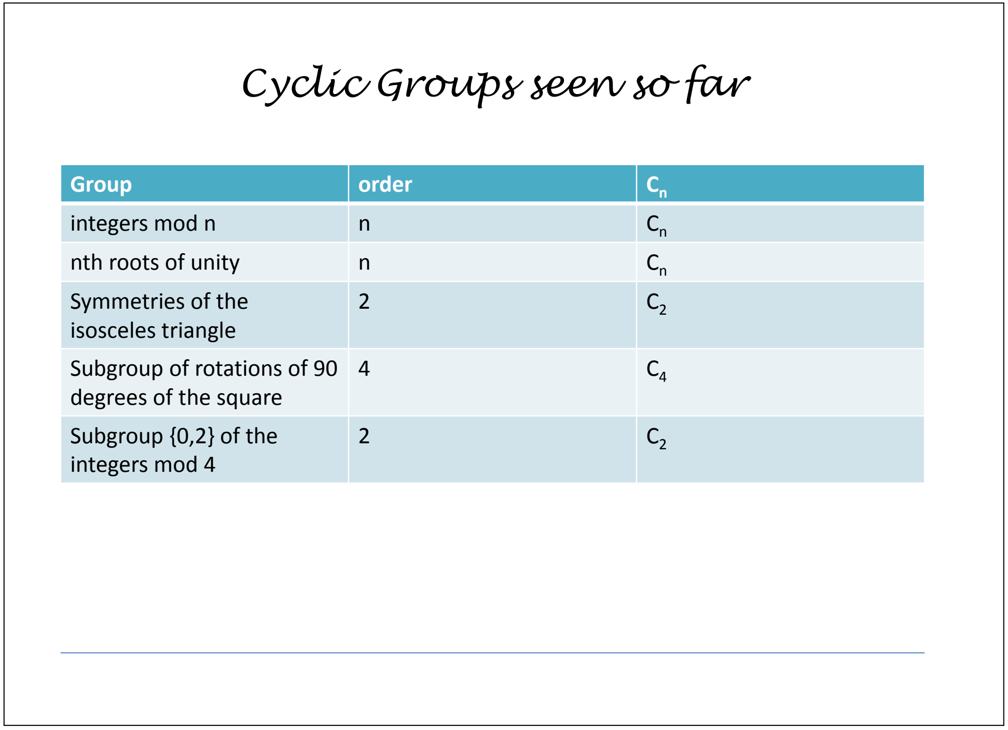
We can summarize the cyclic groups encountered so far:

group	C_n	order n
integers mod n $(+)$	C_n	order n
nth roots of unity $(\cdot)$	C_n	order n
rotations of regular polygons with n sides	C_n	order n
symmetries of isosceles triangles	C_2	order 2
$(\mathbb{Z}, +)$	C_∞	infinite order

Now that we know that cyclic groups are all just instances of the abstract cyclic group C_n for some $n \in \mathbb{N}$ or $n = \infty$, we can ask ourselves how much structure exists in C_n as a function of the properties of the number $n \in \mathbb{N}$. This is important, because every instance of C_n will naturally inherit the structure of C_n! We start with the subgroups of C_n.



Idea of the Proof



Cyclic Groups seen so far

Group	order	C_n
integers mod n	n	C_n
nth roots of unity	n	C_n
Symmetries of the isosceles triangle	2	C_2
Subgroup of rotations of 90 degrees of the square	4	C_4
Subgroup {0,2} of the integers mod 4	2	C_2

Theorem 7. *Subgroups of a cyclic group are cyclic.*

Proof. Let $(G, \cdot)$ be a cyclic group, denoted multiplicatively, finite or infinite. By definition of cyclic, there exists an element $g \in G$ so that $G = \langle g \rangle$. Now let H be a subgroup of G. This means that H contains 1. If $H = \{1\}$, it is a cyclic group of order 1. If H contains more elements, then necessarily, they are all powers of g. Let m be the smallest positive power of g that belongs to H, i.e., $g^m \in H$ (and $g, g^2, \dots, g^{m-1} \notin H$). We must have by closure that $\langle g^m \rangle$ is a subgroup of H. Assume for the sake of contradiction that there exists $g^t \in H, t > m$ and $g^t \notin \langle g^m \rangle$. Then by the Euclidean division algorithm,

$$t = mq + r,\ 0 < r < m - 1.$$

Therefore

$$g^t = g^{mq+r} = g^{mq} g^r \in H,$$

and since g^{mq} is invertible, we get

$$\underbrace{g^{-mq}}_{\in H} \underbrace{g^t}_{\in H} = g^r \Rightarrow g^r \in H.$$

But r is a positive integer smaller than m, which contradicts the minimality of m. This shows that g must belong to $\langle g^m \rangle$ (i.e., $r = 0$) and hence $\langle g^m \rangle$ will contain all elements of the subgroup H, which by definition is cyclic and generated by g. ☐

We next study the order of elements in a cyclic group.

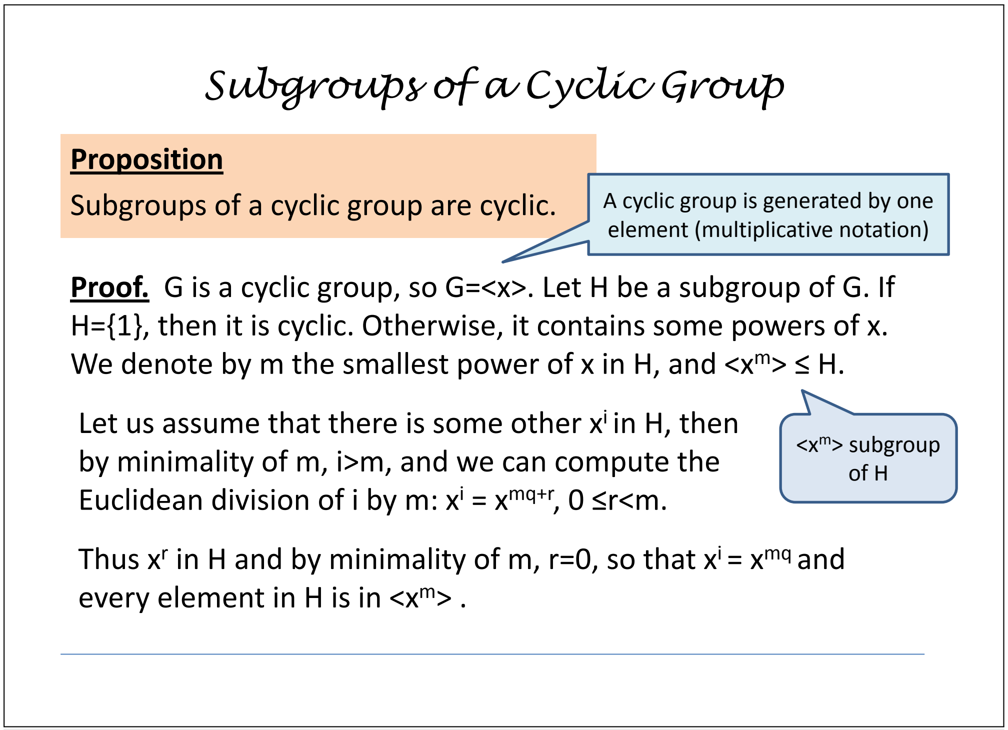
Theorem 8. *In the cyclic group C_n, the order of an element g^k where $\langle g \rangle = C_n$ is given by $|g^k| = n/\gcd(n, k)$.*

Proof. Recall first that g has order n. Let r be the order of g^k. By definition, this means that $(g^k)^r = 1$, and r is the smallest r that satisfies this. Now we need to prove that $r = n/\gcd(n, k)$, which is equivalent to show that (1) $r | \frac{n}{\gcd(n,k)}$ and (2) $\frac{n}{\gcd(n,k)} | r$.

Step 1. We know that $g^{kr} = 1$ and that g has order n. By definition of order, $kr \geq n$. Suppose that $kr > n$, then we apply the Euclidean division algorithm, to find that

$$kr = nq + s,\ 0 \leq s < n \Rightarrow g^{kr} = g^{nq} g^s = g^s \in G$$

and s must be zero by minimality of n. This shows that $\boxed{n \mid rk}$.



Subgroups of a Cyclic Group

Proposition

Subgroups of a cyclic group are cyclic.

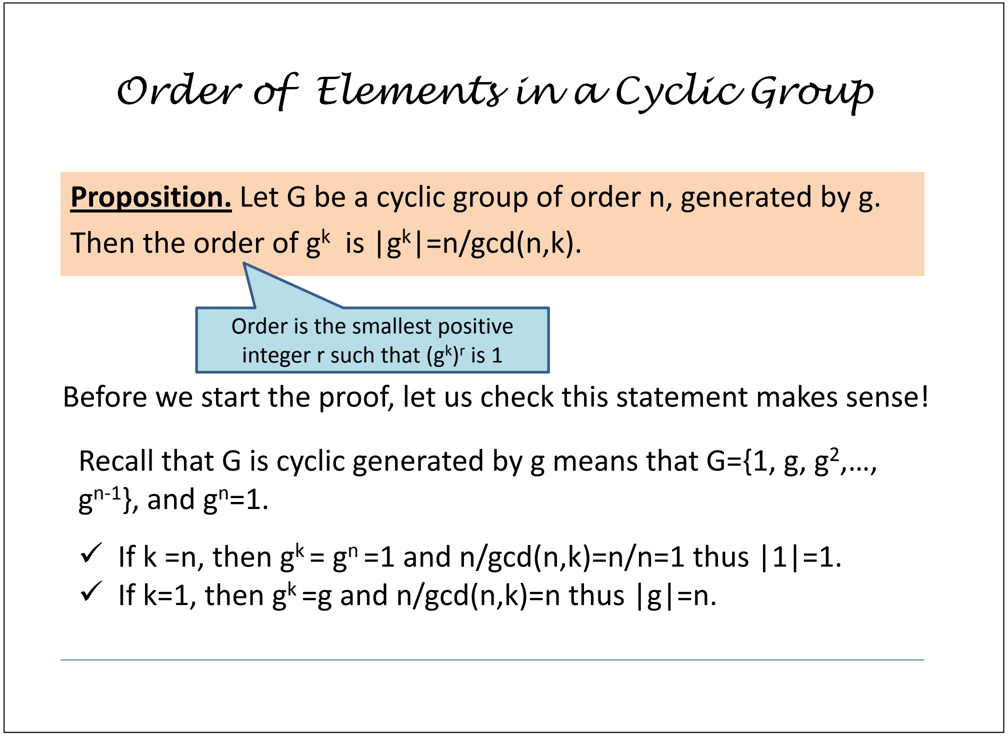
A cyclic group is generated by one element (multiplicative notation)

Proof. G is a cyclic group, so G=<x>. Let H be a subgroup of G. If H={1}, then it is cyclic. Otherwise, it contains some powers of x. We denote by m the smallest power of x in H, and $<x^m> \leq H$.

Let us assume that there is some other x^i in H, then by minimality of m, i>m, and we can compute the Euclidean division of i by m: $x^i = x^{mq+r}$, $0 \leq r<m$.

$<x^m>$ subgroup of H

Thus x^r in H and by minimality of m, r=0, so that $x^i = x^{mq}$ and every element in H is in $<x^m>$.



Order of Elements in a Cyclic Group

Proposition. Let G be a cyclic group of order n, generated by g. Then the order of g^k is $|g^k|=n/\gcd(n,k)$.

Order is the smallest positive integer r such that $(g^k)^r$ is 1

Before we start the proof, let us check this statement makes sense!

Recall that G is cyclic generated by g means that $G=\{1, g, g^2,\ldots, g^{n-1}\}$, and $g^n=1$.

- ✓ If k =n, then $g^k = g^n =1$ and $n/\gcd(n,k)=n/n=1$ thus $|1|=1$.
- ✓ If k=1, then $g^k =g$ and $n/\gcd(n,k)=n$ thus $|g|=n$.

Step 2. Using

$$\gcd(n,k)|n \text{ and } \gcd(n,k)|k,$$

with $n|kr$, we get $\boxed{\frac{n}{\gcd(n,k)}|\frac{k}{\gcd(n,k)}r.}$

Step 3. But $\gcd(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}) = 1$ from which we obtain $\boxed{\frac{n}{gcd(n,k)}|r}$ which conclude the proof of (2)! We are now left with (1), namely show that r must divide $n/\gcd(n,k)$.

Step 4. Note that

$$(g^k)^{n/\gcd(n,k)} = (g^n)^{k/\gcd(n,k)} = 1.$$

Now we know that r is the smallest integer that satisfies $(g^k)^r = 1$ thus $n/\gcd(n,k) \geq r$, and using again the Euclidean division algorithm as we did in Step 1, we must have that

$$\frac{n}{\gcd(n,k)} = qr + s \Rightarrow (g^k)^{\frac{n}{\gcd(n,k)}} = (g^k)^{qr+s}, \quad 0 \leq s < r.$$

This would imply

$$1 = 1 \cdot g^s \Rightarrow s = 0.$$

Hence $\boxed{r|\frac{n}{gcd(n,k)}.}$ □

Example 13. The order of 1 is $|1| = |g^n| = \frac{n}{\gcd(n,n)} = 1$, and the order of g is $|g| = \frac{n}{\gcd(n,1)} = n$.

Combining the fact that a cyclic group of order n has cyclic subgroups generated by its elements $\{g^k\}$, and the fact that the orders of these elements are $|g^k| = n/\gcd(n,k)$, we can prove one more result regarding the order of subgroups in a cyclic group.

Theorem 9. *The order of a (cyclic) subgroup of a group C_n divides the order of the group.*

Proof. We have seen in Theorem 7 that if $G = \langle g \rangle$ and H is a subgroup of G, then

$$H = \langle g^m \rangle$$

for some m. We have also seen in Theorem 8 that $|g^m|$ is $n/\gcd(n,m)$, hence $|H| = |g^m| = \frac{n}{\gcd(n,m)}$. Now by definition,

$$\frac{n}{\gcd(n,m)}|n.$$

□

Proof of the Proposition

- Given g^k, we have to check that its order r is n/gcd(k,n). This is equivalent to show that r| n/gcd(k,n) and n/gcd(k,n) | r.
- Step 1 : g^k has order r means $g^{kr} = 1$, which implies n | kr.

> n is the smallest integer such that $g^n =1$, thus if $g^{kr} =1$, kr>n and by Euclidean division, kr =nq+s, 0 ≤s<n. But then $1=g^{kr}= g^{nq+s} = g^s$ showing that s=0 my minimality of n.

- Step 2: gcd(k,n) |k and gcd(k,n)|n thus n/gcd(k,n) | (k/ gcd(k,n))r.
- Step 3 : n/gcd(k,n) and k/gcd(k,n) are coprime thus n/gcd(k,n)|r.
- Step 4: only left to show that r | n/gcd(k,n). But $(g^k)^{n/gcd(k,n)}=1$ thus r | n/gcd(k,n) [if you understood Step 1, this is the same argument!]

Order of Subgroups in a Cyclic Group

- We have seen: every subgroup of a cyclic group is cyclic, and if G is cyclic of order n generated by g, then g^k has order n/gcd(k,n).
- What can we deduce on the order of subgroups of G?

•Let H be a subgroup of G. Then H is cyclic by the first result.
•Since H is cyclic, it is generated by one element, which has to be some power of g, say g^k.
•Thus the order of H is the order of its generator, that is n/gcd(n,k).

In particular, the order of a subgroup divides the order of the group!

The beauty of these results is that they apply to every instance of the cyclic group C_n. One may work with the integers mod n, with the nth roots of unity, or with the group of rotations of a regular polygon with n sides, it is true for all of them that

- all their subgroups are cyclic as well,
- the order of any of their elements is given by Theorem 8,
- and the size of every of their subgroups divides the order of the group.

If we think of the type of searches we did in the first chapters, where we were looking for subgroups in the Cayley tables, it is now facilitated for cyclic groups, since we can rule out the existence of subgroups which do not divide the order of the group!

Example 14. Let us see how to use Theorem 8, for example with 4rth roots of unity. We know that $-1 = i^2$, thus $n = 4$, $k = 2$, and the order of -1 is

$$\frac{n}{\gcd(n,k)} = \frac{4}{2} = 2,$$

as we know!

Example 15. Let us see how to use Theorem 8, this time with the integers mod 4. Let us be careful here that the notation is additive, with identity element 0. Recall that the integers mod 4 are generated by 1. Now assume that we would like to know the order of 3 mod 4. We know that $k = 3$ and $n = 4$, thus

$$\frac{n}{\gcd(n,k)} = \frac{4}{1} = 4,$$

and indeed

$$3+3 = 6 \equiv 2 \mod 4,\ 3+3+3 = 9 \equiv 1 \mod 4,\ 3+3+3+3 = 12 \equiv 0 \mod 12.$$

This might not look very impressive because these examples are small and can be handled by hand, but these general results hold no matter how big C_n is!

Examples

Thus these results apply to all the cyclic groups we have seen:

- nth roots of unity
- integer mod n
- rotations of 2π/n

4rth root of unity/ Integers mod 4

- We saw that i is a primitive root, thus it generates the cyclic group of 4rth roots of unity.
- To determine the order of -1, we notice that -1= i^2.
- Now we only need to compute n/gcd(n,k)=4/gcd(4,2)=2.

- What is the order of 3 mod4 ?
- We recall that the integers mod 4 are generated by 1.
- Thus 3=k, n=4, and we compute n/gcd(k,n)=4/gcd(3,4)=4.

We will now start thinking the other way round! So far, we saw many examples, and among them, we identified several instances of the cyclic group C_n (integers mod n with addition, nth roots of unity with multiplication, rotations of regular polygons with n sides...). We also saw that C_n exists for every positive integer n. Surely, there are more groups than cyclic groups, because we know that the group of symmetries of the equilateral triangle seen in the exercises (let us call it D_3 where 3 refers to the 3 sides of the triangle) and the group of symmetries of the square (let us call it D_4, where 4 again refers to the 4 sides of the square) are not cyclic, since they are not abelian! (and we proved that a cyclic group is always abelian...) The "D" in D_3 and D_4 comes from the term "dihedral".

order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	
2	C_2	
3	C_3	
4	C_4	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8	D_4

The next natural question is: what are possible other groups out there? To answer this question, we will need more tools.

Definition 13. Let $(G, \cdot)$ be a group and let H be a subgroup of G. We call the set

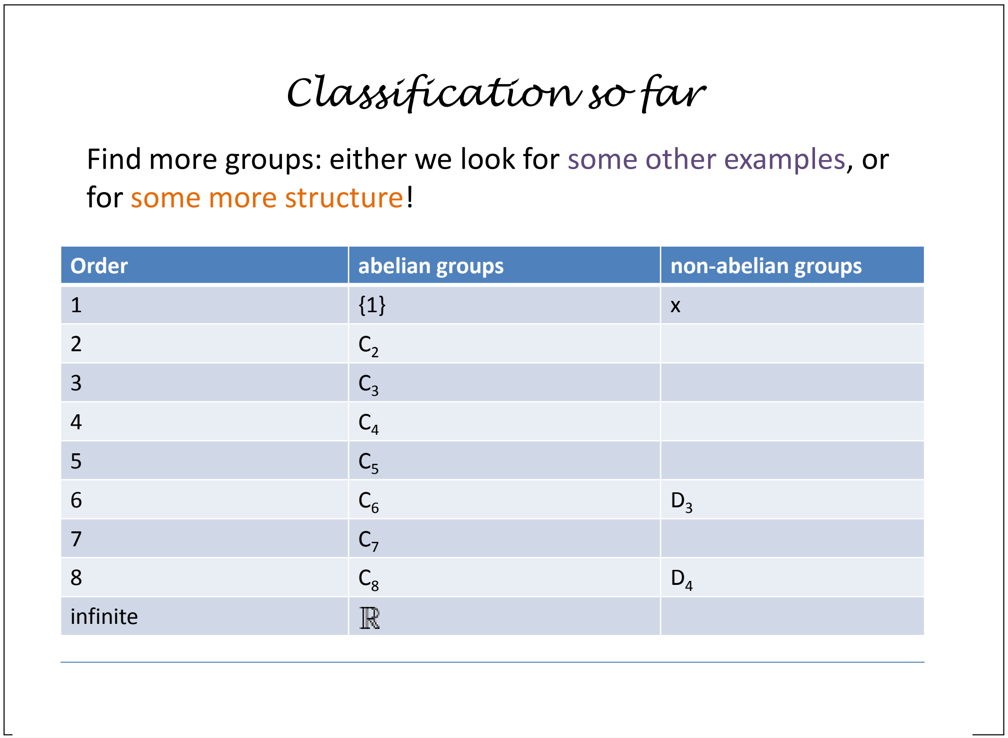
$$gH = \{gh | h \in H\}$$

a left coset of H.

We have that gH is the set of elements of G that we see when we multiply (i.e., combine using the group operation $\cdot$) the specific element $g \in G$ with all the elements of H. Similarly, a right coset of H is given by

$$Hg = \{hg | h \in H\}.$$

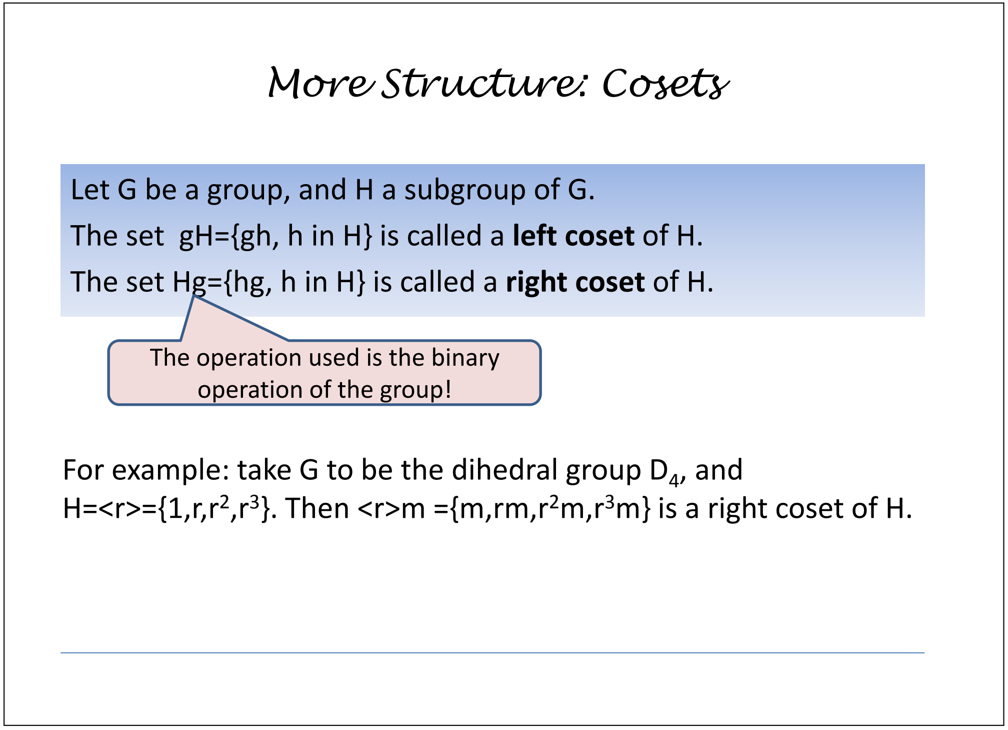
If the group is not abelian, there is a need to distinguish right and left cosets, since they might not be the same set!



Classification so far

Find more groups: either we look for some other examples, or for some more structure!

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	
3	C_3	
4	C_4	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8	D_4
infinite	$\mathbb{R}$	



More Structure: Cosets

Let G be a group, and H a subgroup of G.
The set gH={gh, h in H} is called a **left coset** of H.
The set Hg={hg, h in H} is called a **right coset** of H.

The operation used is the binary operation of the group!

For example: take G to be the dihedral group D_4, and $H=\langle r\rangle=\{1,r,r^2,r^3\}$. Then $\langle r\rangle m=\{m,rm,r^2m,r^3m\}$ is a right coset of H.

It might help to think of a coset as a “translation of a subgroup H” by some element g of the group.

Example 16. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. The coset $1 + H$ is $1 + H = \{1, 3\}$.

Example 17. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. The coset Hm is $Hm = \{m, rm, r^2m, r^3m\}$.

Let us see a few properties of cosets.

Lemma 2. *Let G be a group, and H be a subgroup.*

1. *For every $g \in G$, $g \in gH$ and $g \in Hg$.*
2. *We have $gH = H$ if and only if $g \in H$.*

Proof.

1. Since H is a subgroup, $1 \in H$, hence $g \cdot 1 \in gH$ that is $g \in gH$. Similarly $1 \cdot g \in Hg$ showing that $g \in Hg$.
2. Suppose first that $g \in H$. Then gH consists of elements of H, each of them multiplied by some element g of H. Since H is a subgroup, $gh \in H$ and $gH \subset H$. To show that $H \subseteq gH$, note that

   $$g^{-1}h \in H \Rightarrow g(g^{-1}h) \in gH \Rightarrow h \in gH$$

   for every $h \in H$!
   Conversely, if $gH = H$, then $gh \in H$ for every h, and $g \cdot 1 \in H$.

□

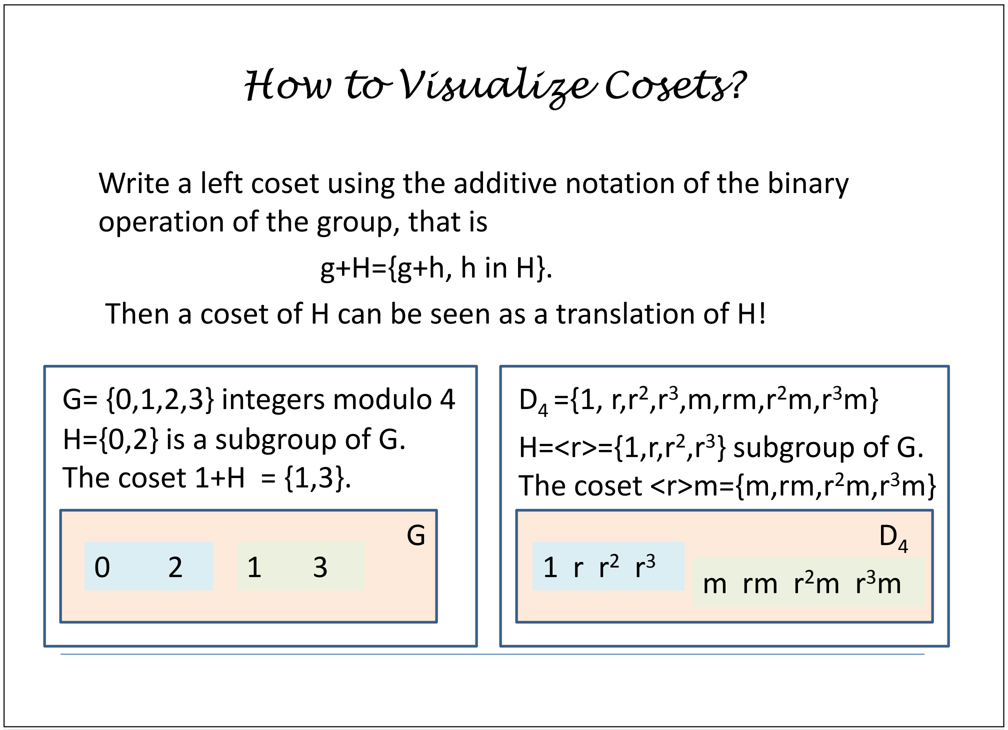
The next lemma tells us when two cosets are the same set!

Lemma 3. *Let G be a group with subgroup H. Then*

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H, \ g_1, g_2 \in G.$$

Proof. If $g_1H = g_2H$, then $\{g_1h | h \in H\} = \{g_2h | h \in H\}$ and there exists an $h \in H$ such that $g_1h = g_2 \cdot 1$, which shows that $h = g_1^{-1}g_2 \in H$.

Conversely, if $g_1^{-1}g_2 \in H$, then $g_1^{-1}g_2 = h \in H$ and $g_2 = g_1h$ which shows that $g_2H = g_1hH = g_1H$, where the last equality follows from the above lemma. □



How to Visualize Cosets?

Write a left coset using the additive notation of the binary operation of the group, that is

$$g+H=\{g+h, h \text{ in } H\}.$$

Then a coset of H can be seen as a translation of H!

$G= \{0,1,2,3\}$ integers modulo 4
$H=\{0,2\}$ is a subgroup of G.
The coset $1+H = \{1,3\}$.

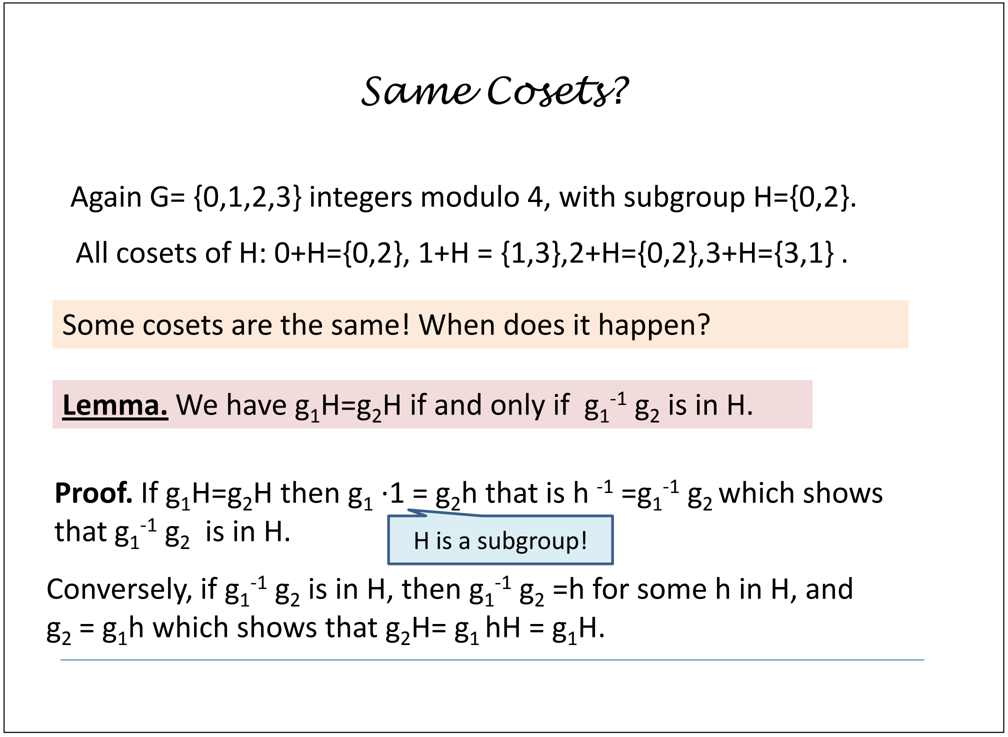
G

0 2 | 1 3

$D_4 =\{1, r,r^2,r^3,m,rm,r^2m,r^3m\}$
$H=<r>=\{1,r,r^2,r^3\}$ subgroup of G.
The coset $<r>m=\{m,rm,r^2m,r^3m\}$

D_4

1 r r^2 r^3 | m rm r^2m r^3m



Same Cosets?

Again $G= \{0,1,2,3\}$ integers modulo 4, with subgroup $H=\{0,2\}$.

All cosets of H: $0+H=\{0,2\}$, $1+H = \{1,3\}$, $2+H=\{0,2\}$, $3+H=\{3,1\}$.

Some cosets are the same! When does it happen?

Lemma. We have $g_1H=g_2H$ if and only if $g_1^{-1} g_2$ is in H.

Proof. If $g_1H=g_2H$ then $g_1 \cdot 1 = g_2h$ that is $h^{-1} =g_1^{-1} g_2$ which shows that $g_1^{-1} g_2$ is in H.

H is a subgroup!

Conversely, if $g_1^{-1} g_2$ is in H, then $g_1^{-1} g_2 =h$ for some h in H, and $g_2 = g_1h$ which shows that $g_2H= g_1 hH = g_1H$.

We next show that cosets of a given subgroup H of G have the property of partitioning the group G. This means that G can be written as a disjoint union of cosets! That

$$G = \bigcup gH$$

comes from the fact that g runs through every element of G (and $g \in gH$), thus the union of all cosets gH will be the group G. To claim that we have a partition, we need to argue that this is a disjoint union, namely that cosets are either identical or disjoint.

Proposition 8. *Let G be a group with subgroup H, and let g_1, g_2 be two elements of G. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.*

Proof. If the intersection of g_1H and g_2G is empty, we are done. So suppose there exists an element g both in g_1H and in g_2H. Then

$$g = g_1h = g_2h'$$

thus

$$g_1hH = g_2h'H \Rightarrow g_1H = g_2H,$$

using Lemma 2. □

Example 18. We continue Example 16. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. The cosets of H are $1 + H = \{1, 3\}$ and $0 + H = \{0, 2\}$. We have

$$G = (1 + H) \cup (0 + H).$$

Example 19. . We continue Example 17. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. The cosets of H are $Hm = \{m, rm, r^2m, r^3m\}$ and $H = \{1, r, r^2, r^3\}$. We have

$$D_4 = Hm \cup H.$$

We need a last property of cosets before proving a fundamental theorem of group theory!

Cosets partition the Group!

Let G be a group, with subgroup H, and take *all the cosets gH* of H.

Since g takes every value in G, and H contains 1, the union of all cosets is the whole group: G= U gH.

We now prove that two cosets g_1H and g_2H are either identical or disjoint!

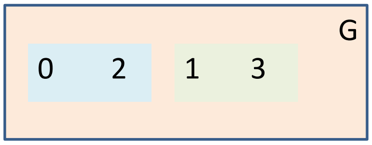
Suppose there exists an element g both in g_1H and in g_2H, then g = g_1h =g_2h'. Thus g_1hH = g_1H = g_2h' H=g_2H.

Cosets partition the Group: Examples

G= {0,1,2,3} integers modulo 4

H={0,2} is a subgroup of G.

The coset 1+H = {1,3}.

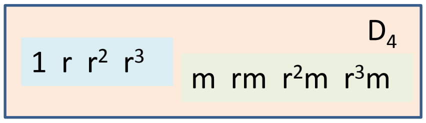


G = {0,2} U {1, 3} = H U (1+H)

D_4 ={1, r,r^2,r^3,m,rm,r^2m,r^3m}

H=<r>={1,r,r^2,r^3} subgroup of G.

The coset <r>m={m,rm,r^2m,r^3m}



D_4 = {1,r,r^2,r^3} U {m rm r^2m r^3m}
= <r> U <r>m

Proposition 9. *Let G be a group with subgroup H. Then*

$$|H| = |gH|, \ g \in G.$$

In words, cosets of H all have the same cardinality.

Proof. To prove that the two sets H and gH have the same number of elements, we define a bijective map (one-to-one correspondence) between their elements. Consider the map:

$$\lambda_g : H \to gH, h \mapsto \lambda_g(h) = gh.$$

This map is injective (one to one): indeed

$$\lambda_g(h_1) = \lambda_g(h_2) \Rightarrow gh_1 = gh_2$$

and since g is invertible, we conclude that $h_1 = h_2$.

This map is surjective (onto): indeed, every element in gH is of the form gh, and has preimage h. □

Example 20. We continue Example 18. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. We have

$$\begin{aligned} |1 + H| &= |\{1, 3\}| = 2 \\ |H| &= |\{0, 2\}|. \end{aligned}$$

Example 21. We continue Example 19. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. We have

$$\begin{aligned} |Hm| &= |\{m, rm, r^2m, r^3m\}| = 4, \\ |H| &= |\{1, r, r^2, r^3\}|. \end{aligned}$$

We are finally ready for Lagrange Theorem!

Cardinality of a Coset

We have $|gH|=|H|$ (the cardinality of a coset of H is the cardinality of H).

The two sets gH and H are in bijection.
Indeed, consider the map λ_g:H→ gH, that sends h to gh.

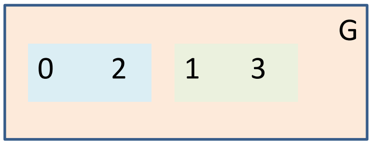
- for every gh in gH, there exists a preimage, given by h.
- if two elements h and h' are mapped to the same element, then gh=gh', and it must be that h=h'.

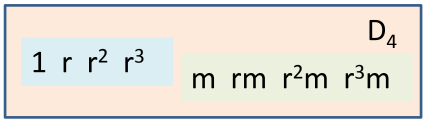
Both steps rely on g being invertible!

Cardinality of a Coset: Examples

G= {0,1,2,3} integers modulo 4
H={0,2} is a subgroup of G.

D_4 ={1, r,r^2,r^3,m,rm,r^2m,r^3m}
H=<r>={1,r,r^2,r^3} subgroup of G.





| H |= |1+H| =2

|<r>| = |<r>m|

Theorem 10. *Let G be a group and H be a subgroup of G. Then*

$$|G| = [G : H]|H|$$

where $[G : H]$ is the number of distinct left (or right) cosets of H in G. If $|G|$ is finite, then

$$[G : H] = \frac{|G|}{|H|}$$

and $|H|$ divides $|G|$.

Note that this also shows that the number of distinct left or right cosets is the same. It is called the index of H in G.

Proof. We know that the cosets of H partition G, that is

$$G = \bigcup_{k=1}^{r} g_k H,$$

where $r = [G : H]$ is the number of distinct cosets of H.

We have also seen that $|gH| = |H|$ in Proposition 9, i.e., all the cosets have the same cardinality as H. Therefore

$$|G| = \sum_{k=1}^{r} |g_k H| = r|H| = [G : H]|H|.$$

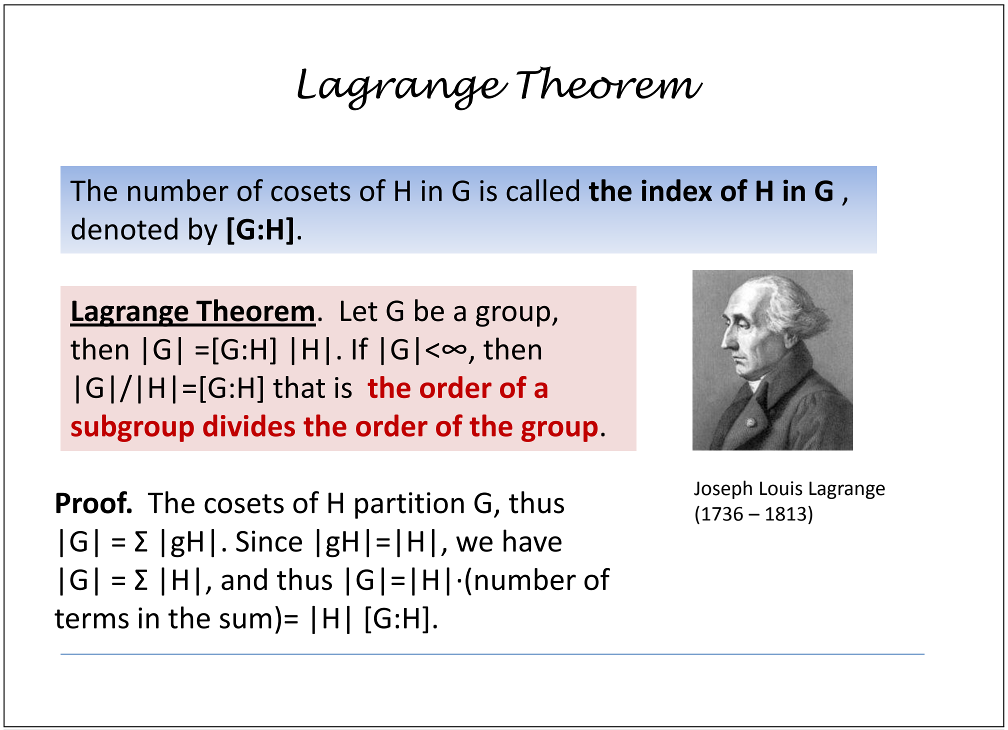
$\square$

Example 22. We finish Example 16. Let G be the group of integers mod 4, and let H be the subgroup $\{0, 2\}$. The cosets of H are $1 + H = \{1, 3\}$ and $0 + H = \{0, 2\}$. Then $[G : H] = 2$ and

$$|G| = [G : H]|H| = 2|H| = 4.$$

Example 23. We also finish Example 17. Let G be the group of symmetries of the square, denoted by D_4, and let H be the subgroup $\{1, r, r^2, r^3\}$ of rotations. The cosets of H are $Hm = \{m, rm, r^2m, r^3m\}$ and $H = \{1, r, r^2, r^3\}$. Then $[G : H] = 2$ and

$$|D_4| = [G : H]|H| = 2|H| = 8.$$



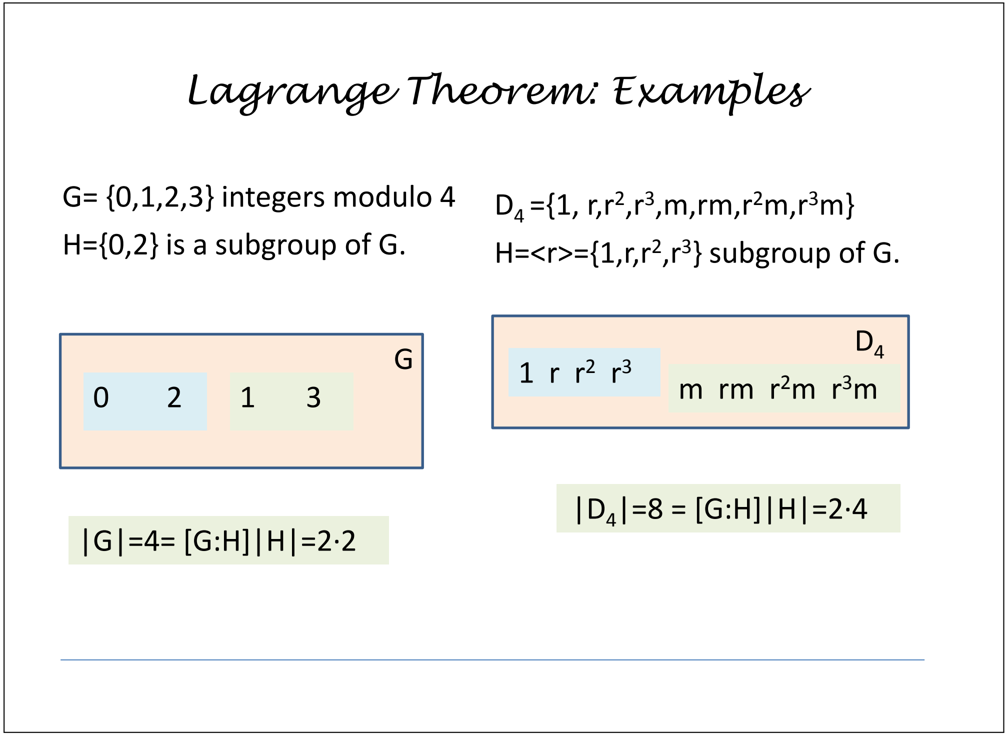
Lagrange Theorem

The number of cosets of H in G is called **the index of H in G** , denoted by **[G:H]**.

Lagrange Theorem. Let G be a group, then $|G| = [G:H]\,|H|$. If $|G|<\infty$, then $|G|/|H|=[G:H]$ that is **the order of a subgroup divides the order of the group**.

Proof. The cosets of H partition G, thus $|G| = \Sigma\,|gH|$. Since $|gH|=|H|$, we have $|G| = \Sigma\,|H|$, and thus $|G|=|H|\cdot$(number of terms in the sum)$= |H|\,[G:H]$.

Joseph Louis Lagrange
(1736 – 1813)



Lagrange Theorem: Examples

G= {0,1,2,3} integers modulo 4
H={0,2} is a subgroup of G.

$D_4 = \{1, r, r^2, r^3, m, rm, r^2m, r^3m\}$
$H=\langle r\rangle=\{1,r,r^2,r^3\}$ subgroup of G.

G
0 2
1 3
D_4
$1\ r\ r^2\ r^3$
$m\ rm\ r^2m\ r^3m$

$|G|=4= [G:H]|H|=2\cdot 2$

$|D_4|=8 = [G:H]|H|=2\cdot 4$

Lagrange Theorem has many consequences.

Corollary 2. *Let G be a finite group. For any $g \in G$, the order $|g|$ of g divides the order of the group $|G|$.*

Proof. Consider the subgroup of G generated by g:

$$\langle g \rangle = \{g, g^2, \cdots, g^{|g|} = 1\}.$$

The order of this subgroup is $|g|$. Hence by Lagrange Theorem, we have

$$|g| \text{ divides } |G|.$$

□

This for example explains why the group of symmetries of the square contains only elements of order 1,2, and 4!

Corollary 3. *A group of prime order is cyclic.*

Proof. Let G be a group of order p, for a prime p. This means elements of G can only have order 1 or p. If g is not the identity element, then g has order p, which shows that G is cyclic. □

Let us now go back to our original question about finding new groups. What we just learnt is that if the order is a prime, then there is only the cyclic group C_p. Thus (boldface means that the classification is over for this order):

order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	**x**
2	C_2	**x**
3	C_3	**x**
4	C_4	
5	C_5	**x**
6	C_6	D_3
7	C_7	**x**
8	C_8	D_4

Corollary 1of Lagrange Theorem

Corollary. Let G be a finite group. The order of an element of G divides the order of the group.

Proof. Let g be an element of G. Then H=<g> is a subgroup of G, with order the order of g (by definition of cyclic group!). Since the order of H divides |G|, the order of g divides |G|.

Example. D_4 ={1, r,r^2,r^3,m,rm,r^2m,r^3m}.
Since |D_4 |=8, elements of D_4 have order 1, 2, 4 (it cannot be 8 because this is not a cyclic group!)

We also know it for cyclic groups! |g^k|=n/gcd(n,k).

Corollary 2 of Lagrange Theorem

Corollary. If |G| is a prime number, then G is a cyclic group.

Proof. If |G| is a prime number p, then we know that the order of an element must divide p, and thus it must be either 1 or p, by definition of prime number. Thus every element g which is not the identity has order p, and G=<g>.

Example. If |G|=3, then G must be the cyclic group C_3.

Since we cannot find any new group of order 2 or 3, let us look at order 4.

We can use a corollary of Lagrange Theorem that tells us that in a group of order 4, elements can have only order 1, 2 or 4.

- If there exists an element of order 4, then we find the cyclic group C_4.
- If there exists no element of order 4, then all elements have order 2 apart the identity. Thus we have a group $G = \{1, g_1, g_2, g_3\}$. Let us try to get the Cayley table of this group. For that, we need to know whether g_1g_2 is the same thing as g_2g_1...But g_1g_2 is an element of G by closure, thus it has order 2 as well:

  $$(g_1g_2)^2 = g_1g_2g_1g_2 = 1 \Rightarrow g_1g_2 = g_2^{-1}g_1^{-1}.$$

  But now, because every element has order 2

  $$g_1^2 = 1 \Rightarrow g_1^{-1} = g_1,\ g_2^2 = 1 \Rightarrow g_2^{-1} = g_2$$

  and we find that

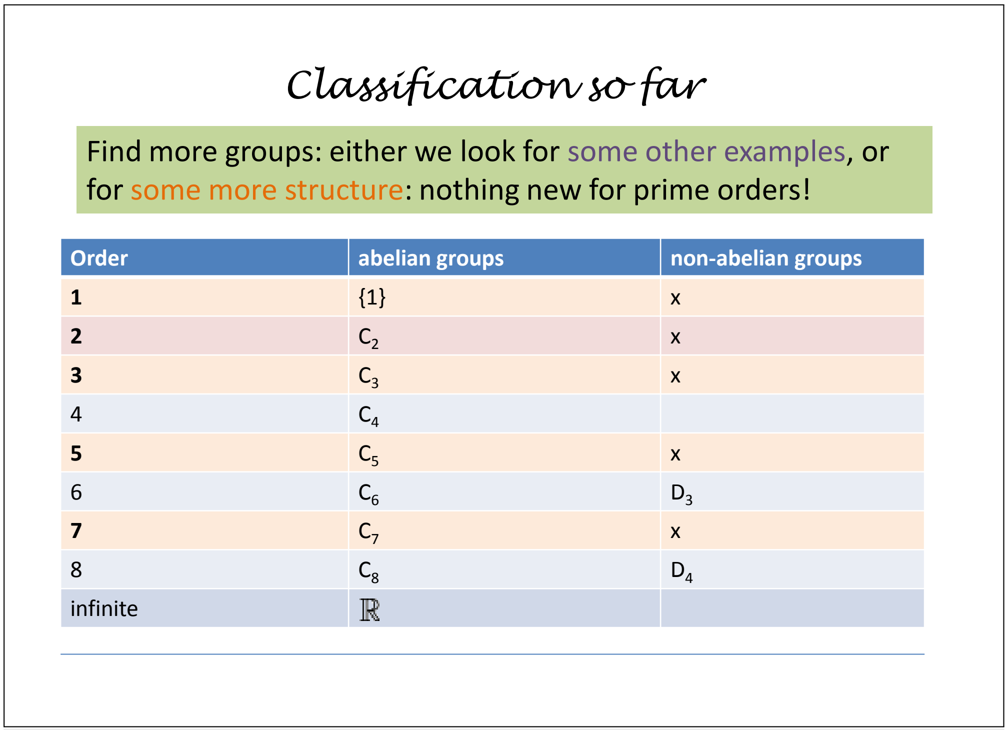
  $$g_1g_2 = g_2g_1.$$

  Furthermore, g_1g_2 is an element of G, which cannot be 1, g_1 or g_2, thus it has to be g_3.

Let us write the Cayley table of the group of order 4 which is not cyclic.

	1	g_1	g_2	g_1g_2
1	1	g_1	g_2	g_1g_2
g_1	g_1	1	g_1g_2	g_2
g_2	g_2	g_1g_2	1	g_1
g_1g_2	g_1g_2	g_2	g_1	1

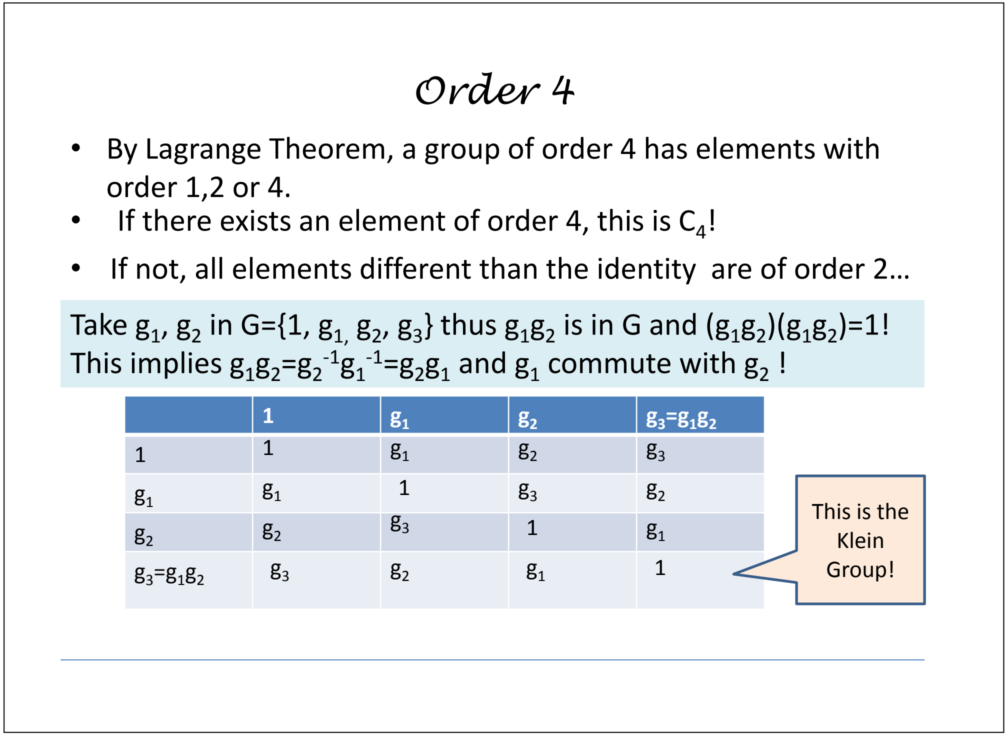
We recognize the table of the symmetries of the rectangle! This group is also called *the Klein group*.



Classification so far

Find more groups: either we look for some other examples, or for some more structure: nothing new for prime orders!

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	x
4	C_4	
5	C_5	x
6	C_6	D_3
7	C_7	x
8	C_8	D_4
infinite	$\mathbb{R}$	



Order 4

- By Lagrange Theorem, a group of order 4 has elements with order 1,2 or 4.
- If there exists an element of order 4, this is C_4!
- If not, all elements different than the identity are of order 2…

Take g_1, g_2 in G={1, g_1, g_2, g_3} thus g_1g_2 is in G and $(g_1g_2)(g_1g_2)=1$!
This implies $g_1g_2=g_2^{-1}g_1^{-1}=g_2g_1$ and g_1 commute with g_2 !

	1	g_1	g_2	$g_3=g_1g_2$
1	1	g_1	g_2	g_3
g_1	g_1	1	g_3	g_2
g_2	g_2	g_3	1	g_1
$g_3=g_1g_2$	g_3	g_2	g_1	1

This is the Klein Group!

We can update our table of small groups:

order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	**x**
2	C_2	**x**
3	C_3	**x**
4	C_4, Klein group	**x**
5	C_5	**x**
6	C_6	D_3
7	C_7	**x**
8	C_8	D_4

Good news: we have progressed in our list of small groups, but we still have not found a group which is not a group of symmetries (up to isomorphism!). We will get back to this question in the next chapter. For now, let us see a few more applications of Lagrange Theorem.

Corollary 4. *Let G be a finite group. Then*

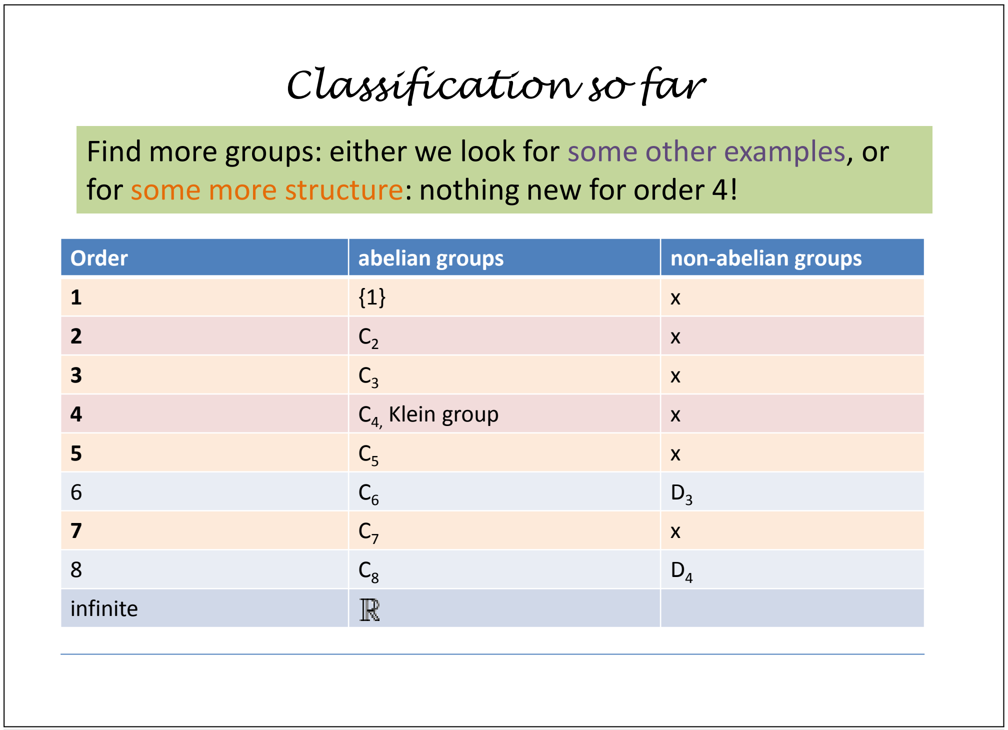
$$g^{|G|} = 1$$

for every $g \in G$.

Proof. We have from Lagrange Theorem that $|g| \mid |G|$, thus $|G| = m|g|$ for some integer m and hence:

$$g^{|G|} = (g^{|g|})^m = 1^m = 1.$$

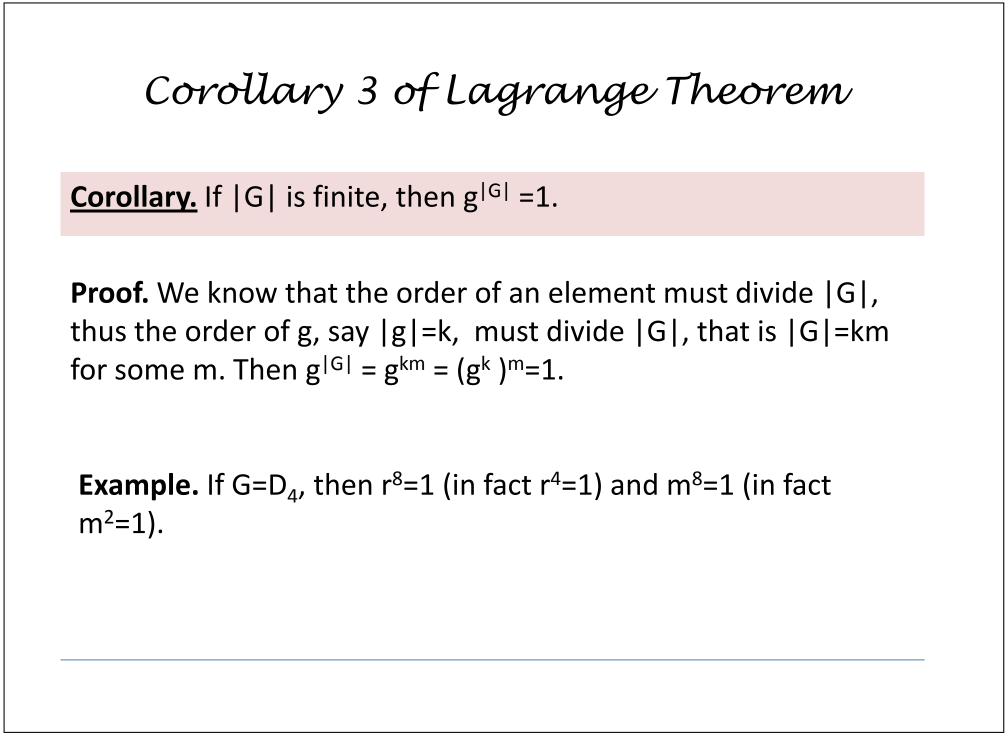
□



Classification so far

Find more groups: either we look for some other examples, or for some more structure: nothing new for order 4!

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	x
4	C_4, Klein group	x
5	C_5	x
6	C_6	D_3
7	C_7	x
8	C_8	D_4
infinite	$\mathbb{R}$	



Corollary 3 of Lagrange Theorem

Corollary. If $|G|$ is finite, then $g^{|G|}=1$.

Proof. We know that the order of an element must divide $|G|$, thus the order of g, say $|g|=k$, must divide $|G|$, that is $|G|=km$ for some m. Then $g^{|G|} = g^{km} = (g^k)^m=1$.

Example. If $G=D_4$, then $r^8=1$ (in fact $r^4=1$) and $m^8=1$ (in fact $m^2=1$).

We continue and prove a result from number theory, known as Euler Theorem.

Theorem 11. *Let a and n be two integers. Then*

$$a^{\varphi(n)} \equiv 1 \mod n$$

if $\gcd(a, n) = 1$.

Proof. If $\gcd(a, n) = 1$, then a is invertible modulo n, and we know that the order of the group of integers mod n under multiplication is $\varphi(n)$. By the previous result

$$a^{|G|} = a^{\varphi(n)} \equiv 1 \mod n.$$

□

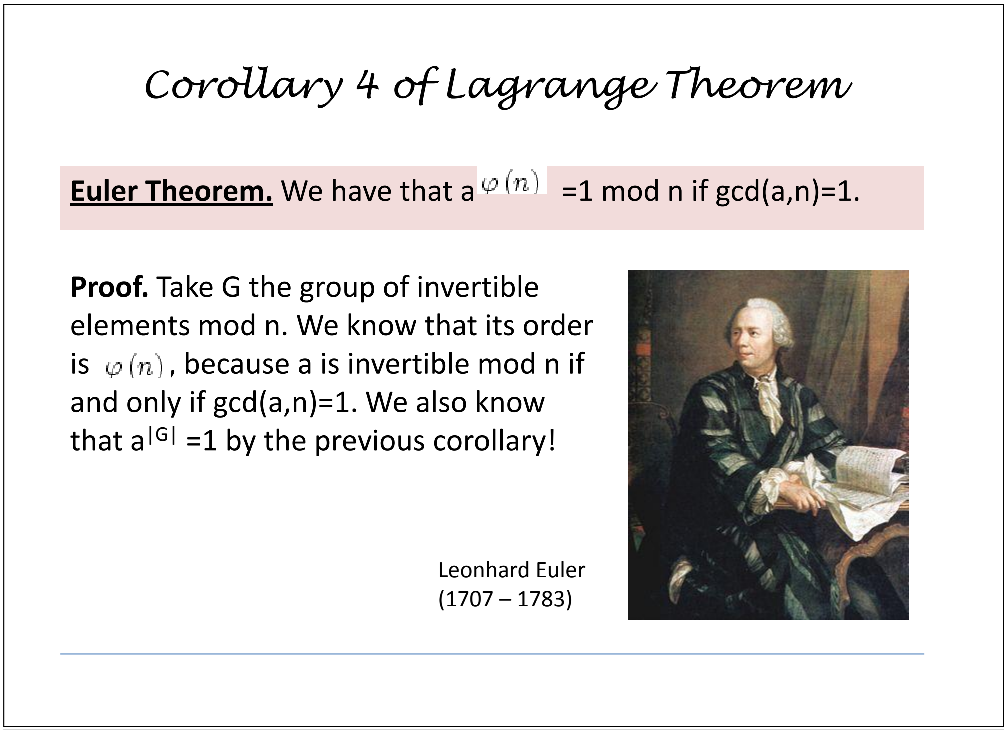
Finally, another nice theorem from number theory is obtained, called **Fermat little theorem**.

Corollary 5. *For every integer a and every prime p, we have $a^p \equiv a$ mod p.*

Proof. Just replace n by a prime p in Euler Theorem, and recall that $\varphi(p) = p - 1$ by definition of $\varphi(p)$. □

The key result of this chapter is really Lagrange Theorem! Thanks to this result and its corollaries, we have learnt a lot about the structure of a group: (1) that the order of a subgroup always divides the order of the group, (2) that the order of an element always divides the order of the group. We also obtained some partial classification of groups of small orders: we showed that for every order we have a cyclic group, and that all the groups we have seen so far are isomorphic to groups of symmetries!

The group structure of integers modulo n, and that of invertible elements modulo n are important in practice in the areas of coding theory and cryptography. A famous example coming from cryptography is the cryptosystem called RSA.

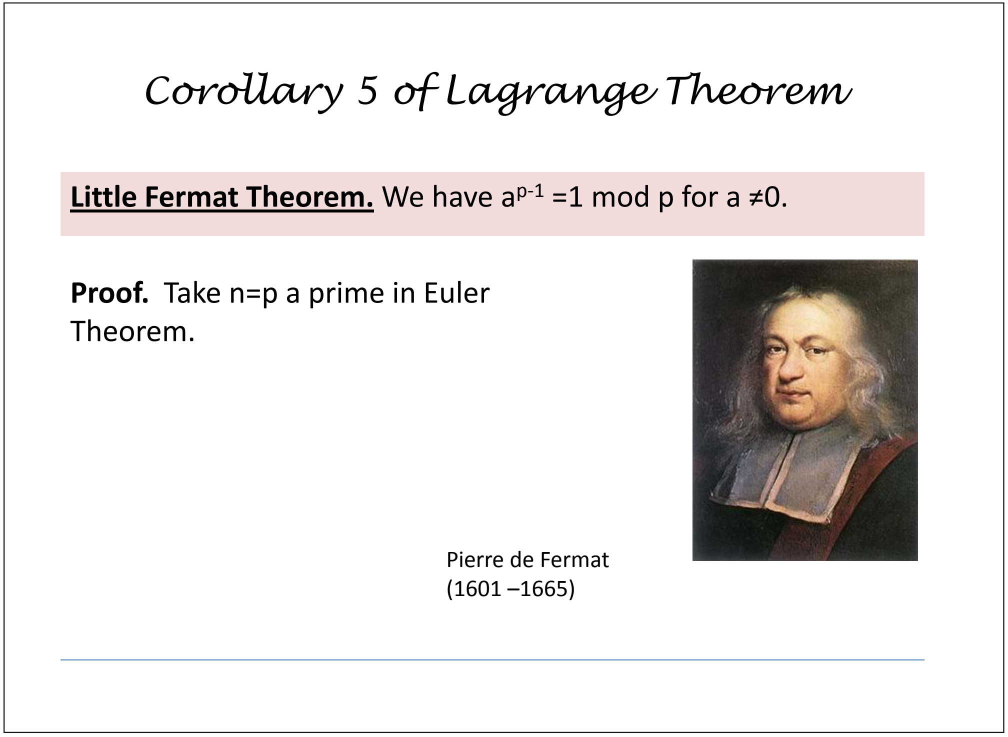


Corollary 4 of Lagrange Theorem

Euler Theorem. We have that $a^{\varphi(n)}$ =1 mod n if gcd(a,n)=1.

Proof. Take G the group of invertible elements mod n. We know that its order is $\varphi(n)$, because a is invertible mod n if and only if gcd(a,n)=1. We also know that $a^{|G|}$ =1 by the previous corollary!

Leonhard Euler
(1707 – 1783)



Corollary 5 of Lagrange Theorem

Little Fermat Theorem. We have a^{p-1} =1 mod p for a ≠0.

Proof. Take n=p a prime in Euler Theorem.

Pierre de Fermat
(1601 –1665)

Exercises for Chapter 5

Exercise 29. Let G be a group and let H be a subgroup of G. Let gH be a coset of H. When is gH a subgroup of G?

Exercise 30. As a corollary of Lagrange Theorem, we saw that the order of an element of a group G divides $|G|$. Now assume that d is an arbitrary divisor of $|G|$. Is there an element g in G with order d?

Exercise 31. Take as group G any group of order 50. Does it contain an element of order 7?

Exercise 32. Take as group G the Klein group of symmetries of the rectangle. Choose a subgroup H of G, write G as a partition of cosets of H, and check that the statement of Lagrange Theorem holds.

Exercise 33. This exercise looks at Lagrange Theorem in the case of an infinite group. Take as group $G = \mathbb{R}$ and as subgroup $H = \mathbb{Z}$. Compute the cosets of H and check that the cosets of H indeed partition G. Also check that the statement of Lagrange Theorem holds.

Chapter 6

Back to Geometry

> *"The noblest pleasure is the joy of understanding."* (Leonardo da Vinci)

At the beginning of these lectures, we studied planar isometries, and symmetries. We then learnt the notion of group, and realized that planar isometries and symmetries have a group structure. After seeing several other examples of groups, such as integers mod n, and roots of unity, we saw through the notion of group isomorphism that most of the groups we have seen are in fact cyclic groups. In fact, after studying Lagrange Theorem, we discovered that groups of prime order are always cyclic, and the only examples of finite groups we have seen so far which are not cyclic are the Klein group (the symmetry group of the rectangle) and the symmetry group of the square. We may define the symmetry group of a regular polygon more generally.

Definition 14. The group of symmetries of a regular n-gon is called the Dihedral group, denoted by D_n.

In the literature, both the notation D_{2n} and D_n are found. We use D_n, where n refers to the number of sides of the regular polygon we consider.

Example 24. If $n = 3$, D_3 is the symmetry group of the equilateral triangle, while for $n = 4$, D_4 is the symmetry group of the square.

Recall so far

- We studied planar isometries.
- We extracted the notion of groups.
- We saw several examples of groups: integer mod n, roots of unity,…
- But after defining group isomorphism, we saw that many of them were just the same group *in disguise*: the cyclic group.

Cyclic groups are nice, but haven't we seen some other groups?

The Dihedral Group D_n

For n >2, the **dihedral group** is defined as the rigid motions of the plane preserving a regular n-gon, with respect to composition.

We saw

- D_3= group of symmetries of the equilateral triangle
- D_4= group of symmetries of the square

(In the literature, the notation D_n and D_{2n} are equally used.)

Recall that the group of symmetries of a regular polygon with n sides contains the n rotations $\{r_\theta,\ \theta = 2\pi k/n,\ k = 0, \dots, n-1\} = \langle r_{2\pi/n} \rangle$, together with some mirror reflections. We center this regular n-sided polygon at $(0, 0)$ with one vertex at $(1, 0)$ (we might scale it if necessary) and label its vertices by the nth roots of unity: $1, \omega, \omega^2, \dots, \omega^{n-1}$, where $\omega = e^{i2\pi/n}$. Now all its rotations can be written in the generic form of planar isometries $H(z) = \alpha z + \beta$, $|\alpha| = 1$ as

$$H(z) = \alpha z,\ \alpha = \omega^k = e^{i2\pi k/n},\ k = 0, \dots, n-1.$$

We now consider mirror reflections about a line l passing through $(0, 0)$ at an angle φ_0, defined by $l(\lambda) = \lambda e^{i\varphi_0}, \lambda \in (-\infty, +\infty)$. To reflect a complex number $z = \rho e^{i\varphi}$ about the line l, let us write $z_R = \rho_R e^{i\varphi_R}$ for the complex number z after being reflected. Since a reflection is an isometry, $\rho_R = \rho$. To compute φ_R, suppose first that $\varphi_R \le \varphi_0$. Then $\varphi_R = \varphi + 2(\varphi_0 - \varphi)$. Similarly if $\varphi_R \ge \varphi_0$, $\varphi_R = \varphi - 2(\varphi - \varphi_0)$, showing that in both cases $\varphi_R = 2\varphi_0 - \varphi$. Hence

$$z_R = \rho e^{i\varphi_R} = \rho e^{i2\varphi_0 - i\varphi} = e^{i2\varphi_0} \rho e^{-i\varphi} = e^{i2\varphi_0} \overline{z}.$$

We now consider not any arbitrary complex number z, but when z is a root of unity ω^k. Mirror reflections that leave $\{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ invariant, that is which map a root of unity to another, will be of the form

$$H(\omega^t) = e^{i\theta} \omega^{-t} = \omega^k$$

where $\theta = 2\varphi_0$ depends on the reflection line chosen. Then $e^{i\theta} = \omega^{k+t} = \omega^{(k+t)_{\text{mod n}}} = \omega^s$, and we find the planar isometries

$$H(z) = \omega^s \overline{z},\ s = 0, 1, \dots, n-1.$$

Hence, given a vertex w^t, there are exactly two maps that will send it to a given vertex w^k: one rotation, and one mirror reflection. This shows that the order of D_n is $2n$.

Furthermore, defining a rotation r and a mirror reflection m by

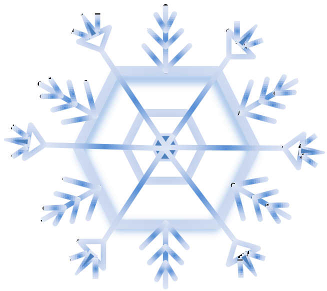
$$r : z \mapsto e^{i2\pi/n} z = \omega z,\ m : z \mapsto \overline{z}$$

we can write all the symmetries of a regular n-gon as

$$D_n = \{r^0 = 1, r, r^2, \dots, r^{n-1}, m, rm, r^m, \dots, r^{n-1}m\}.$$

In particular, $\omega^s \overline{z} = r^s m(z)$.

The Dihedral group D_6



Order of D_n

- We know: isometries of the plane are given by $z \to \alpha z + \beta$ and $z \to \alpha \bar{z} + \beta$, $|\alpha|=1$.
- Thus an element of D_n is either $z \to \alpha z$, or $z \to \alpha \bar{z}$.
- We may write the n vertices of a regular n-gon as nth roots of unity: $1, w, \ldots, w^{n-1}$.
- Now there are exactly 2 maps that send the vertex 1 to say the vertex w^k: $z \to w^k z$, and $z \to w^k \bar{z}$.

Thus the order of D_n is 2n.

These symmetries obey the following rules:

- $r^n = 1$, that is r is of order n, and $\langle r \rangle$ is a cyclic group of order n,
- $m^2 = 1$, that is m is of order 2, as $\overline{\overline{z}} = z$,
- $r^s m$ is also of order 2, as $(r^s m)(r^s m)(z) = \omega^s \overline{\omega^s \overline{z}} = \omega^s \omega^{-s} z = z$.

Since m and $r^s m$ are reflections, they are naturally of order 2, since repeating a reflection twice gives the identity map. Now

$$r^s m r^s m = 1 \Rightarrow m r^s m = r^{-s}, \ \forall s \in \{0, 1, \ldots, n-1\}.$$

The properties

$$r^n = 1, m^2 = 1, mrm = r^{-1}$$

enable us to build the Cayley table of D_n. Indeed $\forall s, t \in \{0, 1, \ldots, n-1\}$

$$r^t r^s = r^{t+s \mod n}, \ r^t r^s m = r^{t+s} m = r^{t+s \mod n} m,$$

and

$$m r^s = r^{-s} m = r^{n-s} m, \ r^t m r^s m = r^t r^{-s} = r^{t-s \mod n}, \ r^t m r^s = r^t r^{-s} m = r^{t-s \mod n} m.$$

We see that D_n is not an Abelian group, since $r^s m \neq m r^s$. Hence we shall write

$$D_n = \{\langle r, m \rangle | m^2 = 1, r^n = 1, mr = r^{-1} m\},$$

that is, the group D_n is generated by r, m via concatenations of r's and m's reduced by the rules $r^n = 1, m^2 = 1, mrm = r^{-1}$ or $mr = r^{-1} m$.

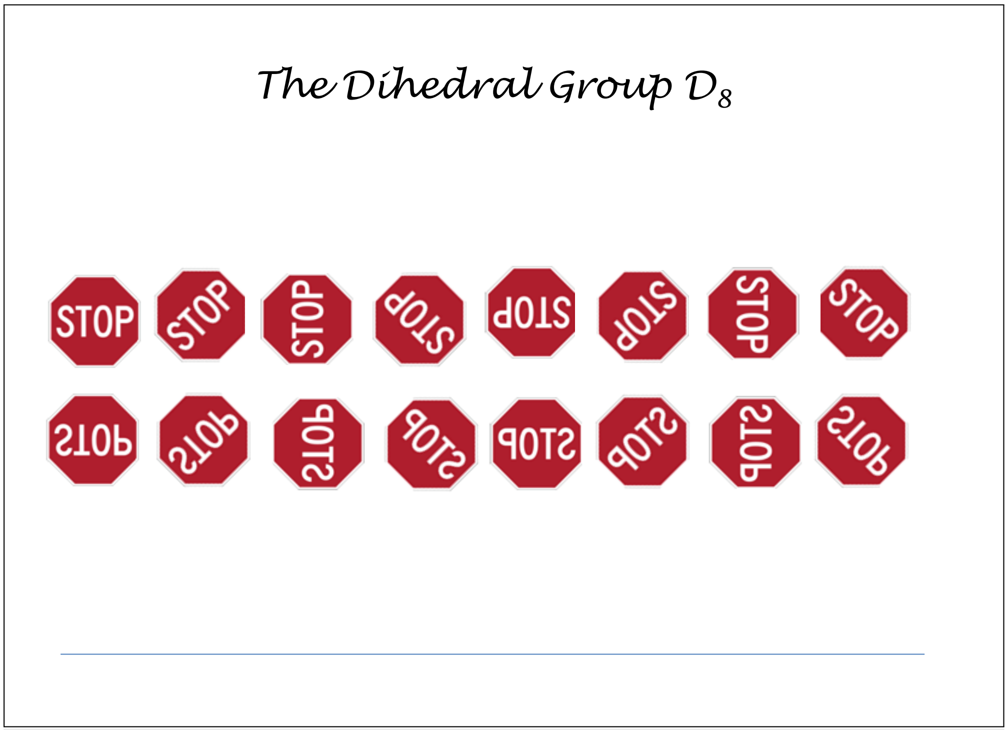
Proof. Consider any string of r's and m's

$$\begin{aligned} &\underbrace{rr \cdot r}_{s_1} \underbrace{mm \cdots m}_{t_1} \underbrace{rr \cdots r}_{s_2} \underbrace{mm \cdots m}_{t_2} \cdots \\ =& r^{s_1} m^{t_1} r^{s_2} m^{t_2} r^{s_3} m^{t_3} \cdots r^{s_k} m^{t_k}. \end{aligned}$$

Due to $m^2 = 1$ and $r^n = 1$ we shall reduce this immediately to a string of

$$r^{\alpha_1} m r^{\alpha_2} m \cdots r^{\alpha_k} m$$

where $\alpha_i \in \{0, 1, \cdots, n-1\}$. Now using $m r^s m = r^{-s}$ gradually reduce all such strings, then we are done. □



The Dihedral Group D_8

Description of the Dihedral Group

- The rotation r:z→ wz generates a cyclic group <r> of order n.
- The reflection m: z→ $\bar{z}$ is in the dihedral group but not in <r>.
- Thus D_n = <r> U <r>m.

$m^2=1$ $m(z)=\bar{z}$ $r(z)=wz$ w root of 1

- Furthermore: $mrm^{-1}(z) = mrm(z) = mr(\bar{z}) = m(w\bar{z}) = \bar{w}z = w^{-1}z = r^{-1}(z)$

That is $mrm^{-1} = r^{-1}$

This shows that: $D_n = \{ \langle r,m \rangle \mid m^2=1, r^n=1, mr = r^{-1}m \}$

Indeed: we know we get 2n terms with <r> and <r>m, and any term of the form mr^i can be reduced to an element in <r> or <r>m using $mr = r^{-1}m$: $mr^i = (mr)r^{i-1} = r^{-1}mr^{i-1} = r^{-1}(mr)r^{i-2}$ etc

What happens if $n = 1$ and $n = 2$? If $n = 1$, we have $r^1 = 1$, i.e., the group D_1 will be $D_1 = \{1, m\}$ with $m^2 = 1$, with Cayley table

	1	m
1	1	m
m	m	1

This is the symmetry group of a segment, with only one reflection or one 180° rotation symmetry.

If $n = 2$ we get $D_2 = \{1, r, m, rm\}$, with Cayley table

	1	r	m	rm
1	1	r	m	rm
r	r	1	rm	m
m	m	rm	1	r
rm	rm	m	r	1

This is the symmetry group of the rectangle, also called the Klein group.

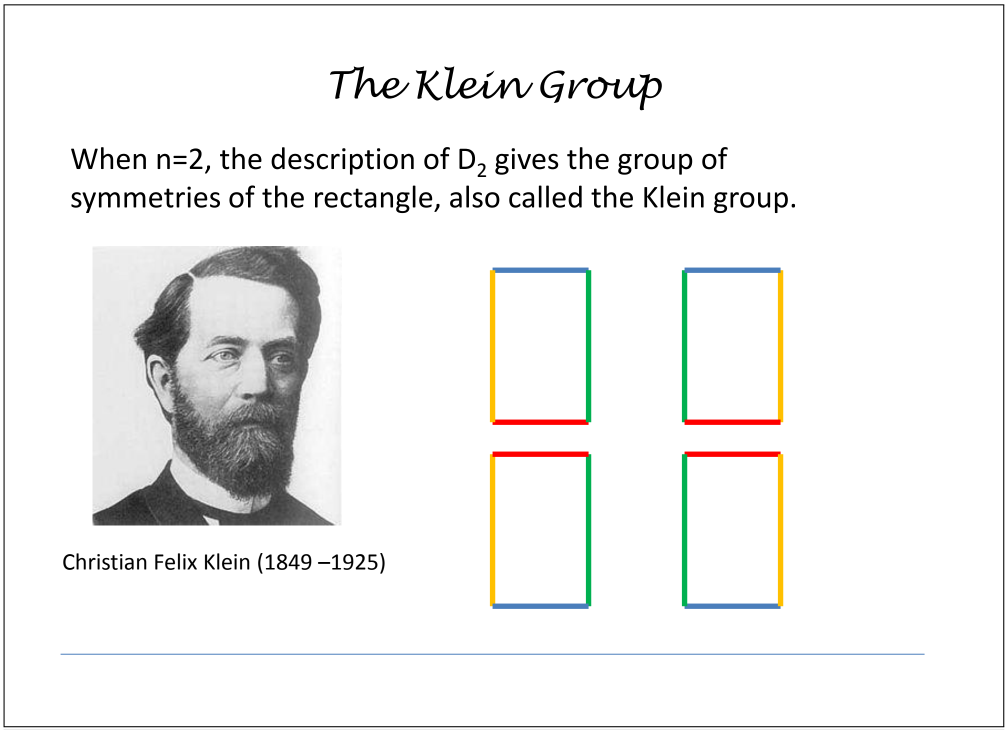
Let us now look back.

- Planar isometries gave us several examples of finite groups:
    1. cyclic groups (rotations of a shape form a cyclic group)
    2. dihedral groups (symmetry group of a regular n-gon)
- Let us remember all the finite groups we have seen so far (up to isomorphism): cyclic groups, the Klein group, dihedral groups.

These observations address two natural questions:

> **Question 1.** Can planar isometries give us other finite groups (up to isomorphism, than cyclic and dihedral groups)?
>
> **Question 2.** Are there finite groups which are not isomorphic to subgroups of planar isometries?

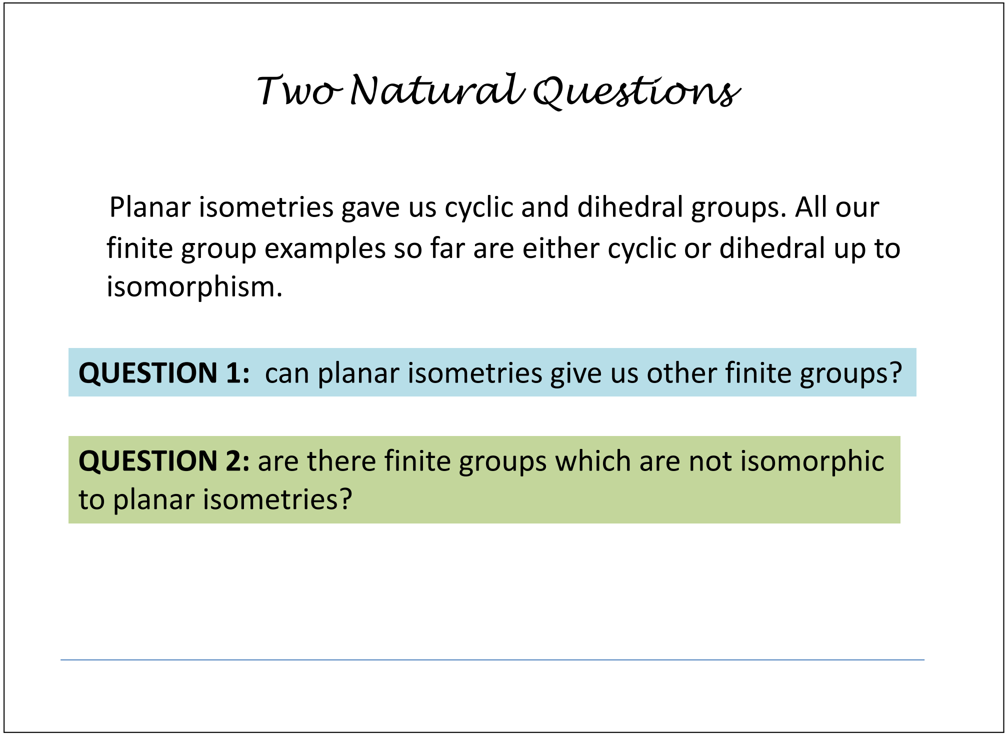
We start with the first question, and study what are all the possible groups that appear as subgroups of planar isometries.



The Klein Group

When n=2, the description of D_2 gives the group of symmetries of the rectangle, also called the Klein group.

Christian Felix Klein (1849 –1925)



Two Natural Questions

Planar isometries gave us cyclic and dihedral groups. All our finite group examples so far are either cyclic or dihedral up to isomorphism.

QUESTION 1: can planar isometries give us other finite groups?

QUESTION 2: are there finite groups which are not isomorphic to planar isometries?

For that, let us recall what we learnt about planar isometries.

From Theorem 1, we know that every isometry in $\mathbb{R}^2$ can be written as $H : \mathbb{C} \to \mathbb{C}$, with

$$H(z) = \alpha z + \beta, \text{ or } H(z) = \alpha \bar{z} + \beta, \ |\alpha| = 1.$$

We also studied fixed points of planar isometries in Exercise 5. If $H(z) = \alpha z + \beta$, then

- if $\alpha = 1$, then $H(z) = z + \beta = z$ and there is no fixed point (apart if $\beta = 0$ and we have the identity map), and this isometry is a translation.
- if $\alpha \neq 1$, then $\alpha z + \beta = z \Rightarrow z = \frac{\beta}{1-\alpha}$, and

  $$H(z) - \frac{\beta}{1-\alpha} = \alpha z + \left(\beta - \frac{\beta}{1-\alpha}\right) = \alpha\left(z - \frac{\beta}{1-\alpha}\right)$$

  showing that $H(z) = \alpha\left(z - \frac{\beta}{1-\alpha}\right) + \frac{\beta}{1-\alpha}$, that is we translate the fixed point to the origin, rotate, and translate back, that is, we have a rotation around the fixed point $\frac{\beta}{1-\alpha}$.

If $H(z) = \alpha\bar{z} + \beta$, we first write this isometry in matrix form as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \tag{6.1}$$

and fixed points (x_F, y_F) of this isometry satisfy the equation

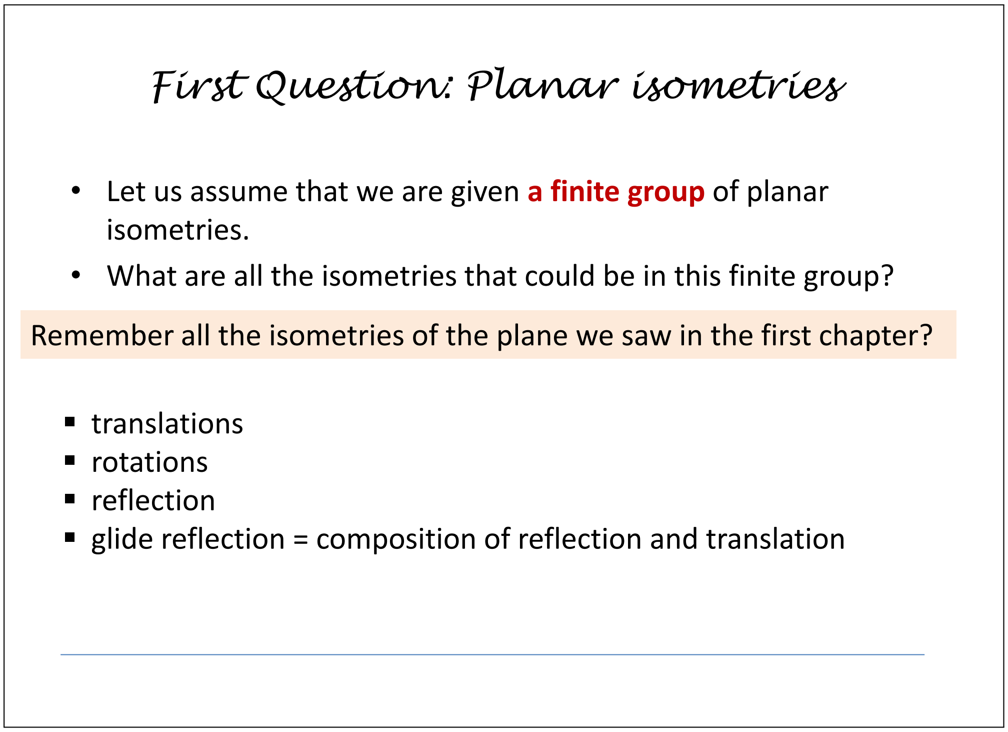
$$\begin{bmatrix} x_F \\ y_F \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} x_F \\ y_F \end{bmatrix} + \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \iff \underbrace{\begin{bmatrix} 1-\cos\theta & -\sin\theta \\ -\sin\theta & 1+\cos\theta \end{bmatrix}}_{M} \begin{bmatrix} x_F \\ y_F \end{bmatrix} = \begin{bmatrix} t_1 \\ t_2 \end{bmatrix}$$

The matrix M has determinant $\det(M) = (1 - cos\theta)(1 + cos\theta) - sin^2\theta = 0$. By rewriting the matrix M as

$$M = \begin{bmatrix} 2sin\frac{\theta}{2}sin\frac{\theta}{2} & -2sin\frac{\theta}{2}cos\frac{\theta}{2} \\ -2sin\frac{\theta}{2}cos\frac{\theta}{2} & 2cos\frac{\theta}{2}cos\frac{\theta}{2} \end{bmatrix} = 2\begin{bmatrix} sin\frac{\theta}{2} \\ -cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} sin\frac{\theta}{2} & -cos\frac{\theta}{2} \end{bmatrix}$$

and fixed points (x_F, y_F) have to be solutions of

$$2\begin{bmatrix} sin\frac{\theta}{2} \\ -cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} sin\frac{\theta}{2} & -cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} x_F \\ y_F \end{bmatrix} = \begin{bmatrix} t_1 \\ t_2 \end{bmatrix}.$$



First Question: Planar isometries

- Let us assume that we are given **a finite group** of planar isometries.
- What are all the isometries that could be in this finite group?

Remember all the isometries of the plane we saw in the first chapter?

- translations
- rotations
- reflection
- glide reflection = composition of reflection and translation

If $[t_1, t_2] = \lambda[\sin(\theta/2), -\cos(\theta/2)]$ then

$$2\langle [x_F, y_F], [\sin(\theta/2), -\cos(\theta/2)]\rangle = \lambda \Rightarrow x_F \sin(\theta/2) - y_F \cos(\theta/2) = \lambda/2$$

showing that (x_F, y_F) form a line, and the isometry (6.1) is now of the form

$$\begin{aligned}\begin{bmatrix} x' \\ y' \end{bmatrix} &= \begin{bmatrix} \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} & 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} \\ 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} & -\cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \lambda \begin{bmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{bmatrix} \\ &= \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \lambda \begin{bmatrix} \sin\frac{\theta}{2} \\ -\cos\frac{\theta}{2} \end{bmatrix}\end{aligned}$$

Multiplying both sides by the matrix (rotation): $\begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{bmatrix}$ we get

$$\underbrace{\begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix}}_{\begin{bmatrix} \tilde{x}' \\ \tilde{y}' \end{bmatrix}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \underbrace{\begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}}_{\begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix}} + \lambda \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and in the rotated coordinates $(\tilde{x}', \tilde{y}')$ and $(\tilde{x}, \tilde{y})$, we have $\tilde{x}' = \tilde{x}$ and $(\tilde{y}' - \frac{\lambda}{2}) = -(\tilde{y} - \frac{\lambda}{2})$ which shows that in the rotated coordinates this isometry is simply a reflection about the line $y = +\frac{\lambda}{2}$.

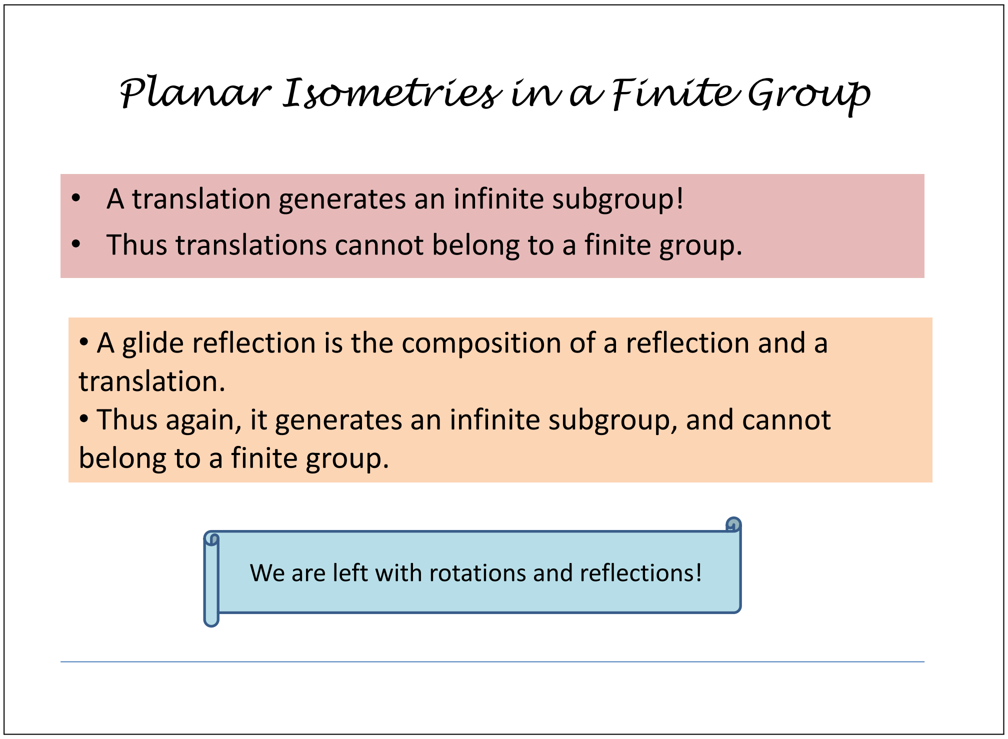
If $[t_1, t_2] \neq \lambda[\sin(\theta/2), -\cos(\theta/2)]$, then we have no fixed points. Just like in the previous analysis we have here

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} cos\frac{\theta}{2} & sin\frac{\theta}{2} \\ sin\frac{\theta}{2} & -cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} t_1 \\ t_2 \end{bmatrix}$$

and we have as before in the rotated coordinates that

$$\begin{bmatrix} \tilde{x}' \\ \tilde{y}' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} + \begin{bmatrix} cos\frac{\theta}{2} & sin\frac{\theta}{2} \\ sin\frac{\theta}{2} & -cos\frac{\theta}{2} \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \quad = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} + \begin{bmatrix} m \\ n \end{bmatrix}$$

and we recognize a translation along the direction of the reflection line $\tilde{x}' = \tilde{x} + m$ and a reflection about the line $y = \frac{n}{2}$, since $(\tilde{y}' - \frac{n}{2}) = -(\tilde{y} - \frac{n}{2})$. This gives a proof of Theorem 2, which we recall here.



Planar Isometries in a Finite Group

- A translation generates an infinite subgroup!
- Thus translations cannot belong to a finite group.

• A glide reflection is the composition of a reflection and a translation.
• Thus again, it generates an infinite subgroup, and cannot belong to a finite group.

We are left with rotations and reflections!

Theorem 12. *Any planar isometry is either*

a) *A rotation about a point in the plane*

b) *A pure translation*

c) *A reflection about a line in the plane*

d) *A reflection about a line in the plane and a translation along the same line (glide reflection)*

Since we are interesting in subgroups of planar isometries, we now need to understand what happens when we compose isometries, since a a finite subgroup of isometries must be closed under composition.

A translation $T(\beta)$ is given by $T(\beta) : z \to z + \beta$, thus

$$T(\beta_2) \circ T(\beta_1) = (z + \beta_1) + \beta_2 = z + \beta_1 + \beta_2 = T(\beta_1 + \beta_2)$$

and translations form a subgroup of the planar isometries that is isomorphic to $(\mathbb{C}, +)$ or $(\mathbb{R}^2, +)$. The isomorphism f is given by $f : T(\beta) \mapsto \beta$.

A rotation R_Ω about a center $\Omega = z_0$ is given by

$$R_\Omega(\theta)z \to e^{i\theta}(z - z_0) + z_0,$$

thus

$$R_\Omega(\theta_2) \circ R_\Omega(\theta_1) = e^{i\theta_2}(e^{i\theta_1}(z - z_0) + z_0 - z_0) + z_0 = R_\Omega(\theta_1 + \theta_2)$$

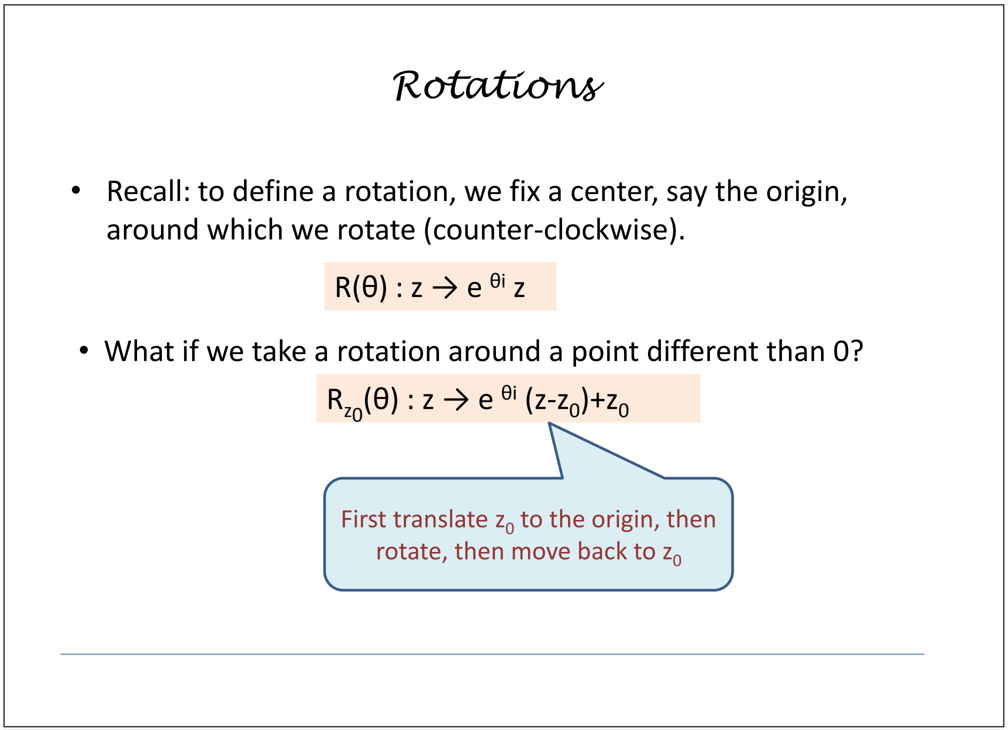
which shows that rotations about a given fixed center $\Omega(= z_0)$ form a subgroup of the group of planar isometries.

We consider now the composition of two rotations about different centers:

$$R_{\Omega_1}(\theta_1) = e^{i\theta_1}(z - z_1) + z_1,\ R_{\Omega_2}(\theta_2) = e^{i\theta_2}(z - z_2) + z_2$$

so that

$$\begin{aligned} R_{\Omega_2}(\theta_2) \circ R_{\Omega_1}(\theta_1) &= e^{i\theta_2}(e^{i\theta_1}(z - z_1) + z_1 - z_2) + z_2 \\ &= e^{i(\theta_2+\theta_1)}(z - z_1) + e^{i\theta_2}(z_1 - z_2) + z_2 \\ &= e^{i(\theta_1+\theta_2)}[z - \gamma] + \gamma \end{aligned}$$



Rotations

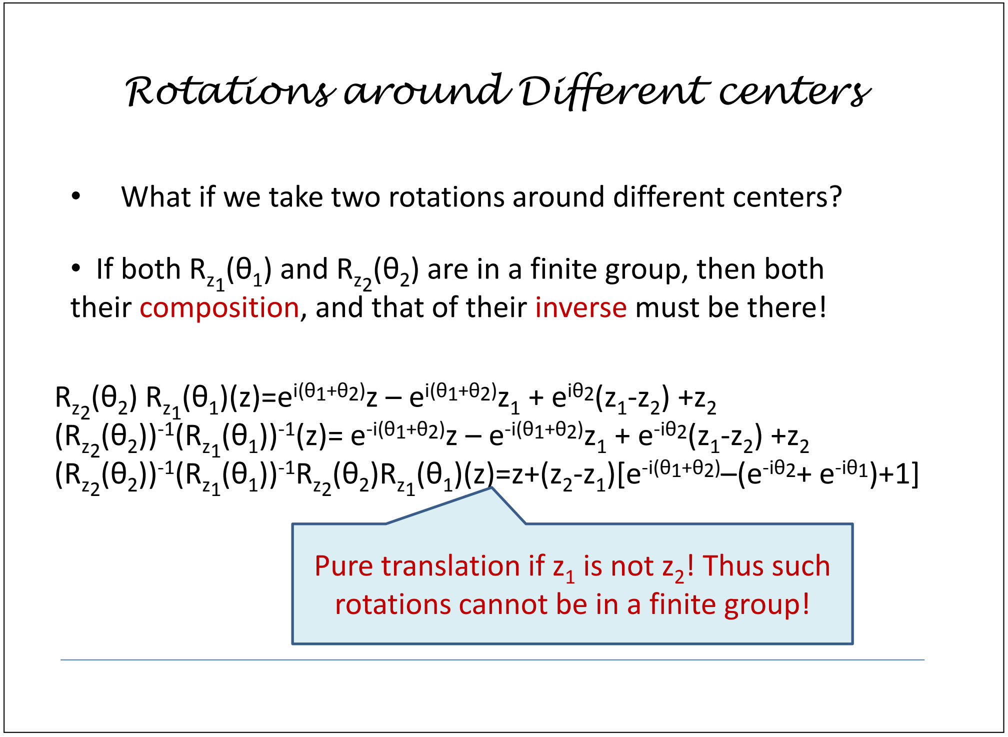
- Recall: to define a rotation, we fix a center, say the origin, around which we rotate (counter-clockwise).

$R(\theta) : z \to e^{\theta i} z$

- What if we take a rotation around a point different than 0?

$R_{z_0}(\theta) : z \to e^{\theta i} (z-z_0)+z_0$

First translate z_0 to the origin, then rotate, then move back to z_0



Rotations around Different centers

- What if we take two rotations around different centers?

- If both $R_{z_1}(\theta_1)$ and $R_{z_2}(\theta_2)$ are in a finite group, then both their composition, and that of their inverse must be there!

$R_{z_2}(\theta_2)\ R_{z_1}(\theta_1)(z)=e^{i(\theta_1+\theta_2)}z - e^{i(\theta_1+\theta_2)}z_1 + e^{i\theta_2}(z_1-z_2) +z_2$

$(R_{z_2}(\theta_2))^{-1}(R_{z_1}(\theta_1))^{-1}(z)= e^{-i(\theta_1+\theta_2)}z - e^{-i(\theta_1+\theta_2)}z_1 + e^{-i\theta_2}(z_1-z_2) +z_2$

$(R_{z_2}(\theta_2))^{-1}(R_{z_1}(\theta_1))^{-1}R_{z_2}(\theta_2)R_{z_1}(\theta_1)(z)=z+(z_2-z_1)[e^{-i(\theta_1+\theta_2)}-(e^{-i\theta_2}+ e^{-i\theta_1})+1]$

Pure translation if z_1 is not z_2! Thus such rotations cannot be in a finite group!

where we determine γ:

$$\begin{aligned} -e^{i(\theta_1+\theta_2)}z_1+e^{i\theta_2}z_1 - e^{i\theta_2}z_2 + z_2 &= -e^{i(\theta_1+\theta_2)}\gamma + \gamma \\ (1-e^{i(\theta_1+\theta_2)})\gamma &= z_2 + e^{i\theta_2}(z_1-z_2) - e^{i(\theta_1+\theta_2)}z_1 \\ \gamma &= \frac{z_2 + e^{i\theta_2}(z_1-z_2) - e^{i(\theta_1+\theta_2)}z_1}{1-e^{i(\theta_1+\theta_2)}} \end{aligned}$$

Hence, we have a rotation by $(\theta_1+\theta_2)$ about a new center γ.

If $z_1 \neq z_2$ and $\theta_2 = -\theta_1$, we get in fact a translation:

$$\begin{aligned} R_{\Omega_2}(-\theta_1) \circ R_{\Omega_1}(\theta_1) &= z - z_1 + e^{-i\theta_1}(z_1-z_2) + z_2 \\ &= z + \underbrace{(z_1-z_2)(e^{-i\theta_1}-1)}_{\text{a translation!}} \end{aligned}$$

After rotations and translations, we are left with reflections and glide reflections about a line l. Suppose we have two reflections, or two glide reflections, of the form

$$\varphi_1 : z \to e^{i\theta_1}\bar{z} + \beta_1, \varphi_2 : z \to e^{i\theta_2}\bar{z} + \beta_2,$$

so that

$$\varphi_2 \circ \varphi_1(z) = e^{i\theta_2}(\overline{e^{i\theta_1}\overline{z} + \beta_1}) + \beta_2 = e^{i(\theta_2-\theta_1)}z + \overline{\beta_1}e^{i\theta_2} + \beta_2.$$

Hence if $\theta_2 = \theta_1 = \theta$ we get a translation:

$$\varphi_2 \circ \varphi_1(z) = z + \underbrace{\overline{\beta_1}e^{i\theta} + \beta_2}_{\text{a translation vector}}$$

which is happening when the lines defining the reflections and glide reflections are parallel (reflect a shape with respect to a line, and then again with respect to another line parallel to the first one, and you will see that the shape is translated in the direction perpendicular to the lines.)

If instead $\theta_2 - \theta_2 \neq 0$, we get a rotation, since the $\varphi_2 \circ \varphi_1(z)$ will have one well defined **fixed point**, given by

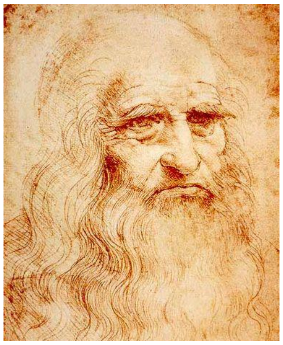
$$\begin{aligned} z_{FP} &= e^{i(\theta_2-\theta_2)}z_{FP} + \overline{\beta_1}e^{i\theta_2} + \beta_2 \\ \Rightarrow z_{FP} &= \frac{\overline{\beta_1}e^{i\theta_2} + \beta_2}{1-e^{i(\theta_2-\theta_1)}} \end{aligned}$$

Reflections

- Among the planar isometries, so far, **only rotations with same center z_0** are allowed!
- **Reflections** are also allowed, assuming that their lines intersect at z_0 (otherwise, we could get rotations about a different point.)

First Question: Leonardo Theorem

QUESTION 1: can planar isometries give us other finite groups than cyclic and dihedral groups?



ANSWER: No! This was already shown by Leonardo da Vinci!

Leonardo da Vinci (1452-1519) `` painter, sculptor, architect, musician, scientist, mathematician, engineer, inventor, anatomist, geologist, cartographer, botanist and writer “ (dixit wikipedia)

Now, we have built up enough prerequisites to prove the following result.

Theorem 13 (Leonardo Da Vinci)**.** *The only finite subgroups of the group of planar symmetries are either C_n (the cyclic group of order n) or D_n (the dihedral group of order $2n$).*

Proof. Suppose that we have a finite subgroup $G = \{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ of the group of planar isometries. This means that for every φ_k, $\langle \varphi_k \rangle$ is finite, that there exists $\varphi_k^{-1} \in G$, and that $\varphi_k \circ \varphi_l = \varphi_s \in G = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$. Thus

1. φ_k cannot be a translation, since $\langle \varphi_k \rangle = \{\varphi_k^n, n \in \mathbb{Z}\}$ is not a finite set.
2. φ_k cannot be a glide reflection, since $\varphi_k \circ \varphi_k$ is a translation hence $\langle \varphi_k^2 \rangle$ is then not a finite set.
3. φ_k and φ_r cannot be rotations about different centers, since

$$\begin{aligned} R_{\Omega_2}(\theta_2)R_{\Omega_1}(\theta_1) &= e^{i(\theta_2+\theta_1)}z - e^{i(\theta_2+\theta_1)}z_1 + e^{i\theta_2}(z_1 - z_2) + z_2 \\ R^{-1}_{\Omega_2}(\theta_2)R^{-1}_{\Omega_1}(\theta_1) &= e^{-i(\theta_2+\theta_1)}z - e^{-i(\theta_2+\theta_1)}z_1 + e^{-i\theta_2}(z_1 - z_2) + z_2 \end{aligned}$$

and

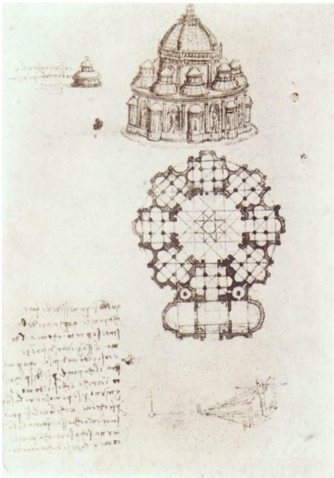
$$\begin{aligned} &R_{\Omega_2}(-\theta_2)R_{\Omega_1}(-\theta_1)R_{\Omega_2}(\theta_2)R_{\Omega_1}(\theta_1) \\ &= e^{-i(\theta_2+\theta_1)}[e^{i(\theta_2+\theta_1)}z - e^{i(\theta_2+\theta_1)}z_1 + e^{i\theta_2}(z_1 - z_2) + z_2] \\ &\quad - e^{-i(\theta_2+\theta_1)}z_1 + e^{-i\theta_2}(z_1 - z_2) + z_2 \\ &= z - z_1 + e^{-i\theta_1}(z_1 - z_2) + e^{-i(\theta_2+\theta_1)}z_2 - e^{-i(\theta_2+\theta_1)}z_1 + e^{-i\theta_2}(z_1 - z_2) + z_2 \\ &= z + (z_2 - z_1) + e^{-i(\theta_2+\theta_1)}(z_2 - z_1) - (z_2 - z_1)(e^{-i\theta_1} + e^{i\theta_2}) \\ &= z + \underbrace{(z_2 - z_1)[e^{-i(\theta_2+\theta_1)} - (e^{-i\theta_2} + e^{-i\theta_1}) + 1]}_{\text{a pure translation if } z_1 \neq z_2} \end{aligned}$$

Therefore in the subgroup $G = \{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ of finitely many isometries, we can have

1) rotations (which must all have the same center Ω)

2) reflections (but their lines must intersect at Ω otherwise we would be able to produce rotations about a point different from Ω and hence produce translations contradicting the finiteness of the set.)

Motivation for Leonardo Theorem



Leonardo da Vinci systematically determined all **possible symmetries** of a central building, and how to attach chapels and niches without destroying its symmetries.

Extract of Leonardo’s notebooks.

Proof of Leonardo Theorem (I)

- We have already shown that a finite group of planar isometries can contain only rotations around the same center, and reflections through lines also through that center.
- Among all the rotations, take the one with smallest strictly positive angle θ, which generates a **finite cyclic group of order say n**, and every rotation belongs to this cyclic group!
- [if θ’ is another rotation angle, then it is bigger than θ, thus we can decompose this rotation between a rotation of angle (a multiple of) θ and a smaller angle, a contradiction] ← same argument as we did several times for cyclic groups!

Let us look at the rotations about Ω in the subgroup $G = \{\varphi_1, \varphi_2, \cdots, \varphi_n\}$ and list the rotation angles (taken in the interval $[0, 2\pi)$) in increasing order:$\theta_1 < \theta_2 < \cdots < \theta_{l-1}$. Now $r(\theta_1)$ is the smallest rotation, and $r(2\theta_1)$, $r(3\theta_1)$,. . .,$r(k\theta_1)$ for all $k \in \mathbb{Z}$ must be in the subgroup as well.

We shall prove that these must be all the rotations in G, i.e., there cannot be a θ_t which is not $k\theta_1 \mod 2\pi$ for some k. Assume for the sake of contradiction that $\theta_t \neq k\theta_1$. Then $\theta_t = s\theta_1 + \zeta$ where $0 < \zeta < \theta_1$, and

$$r(\theta_t)r(-s\theta_1) = r(\theta_t)r(\theta_1)^{-s} = r(\zeta)$$

but $r(\theta_t)r(\theta_1)^{-s}$ belongs to the group of rotations and thus it is a rotation of an angle that belongs to $\{\theta_1, \theta_2, \cdots, \theta_{l-1}\}$, with $\zeta < \theta_1$ contradicting the assumption that θ_1 is the minimal angle.

Also note that $\theta_1 = 2\pi/l$ since otherwise $l\theta_1 = 2\pi + \eta$ with $\eta < \theta_1$ and $r^l(\theta_1) = r(\eta)$ with $\eta < \theta_1$, again contradicting the minimality of θ_1.

Therefore we have exactly l rotations generated by $r(\theta_1)$ and $\langle r(\theta_1)\rangle$ is the cyclic group C_l of order l.

If $C_l = \langle r(\theta_1)\rangle$ exhausts all the elements of $G = \{\varphi_1, \varphi_2, \cdots, \varphi_n\}$, we are done. If not, there are reflections in G too. Let m be a reflection that belongs to $\{\varphi_1, \varphi_2, \ldots, \varphi_n\}$. If m and $\langle r(\theta_1)\rangle$ are both in G, then by closure

$$m, mr, mr^2, \ldots, mr^{p-1} \in G$$

and all these are (1) reflections since $mr^\alpha = r^\beta \Rightarrow m = r^{(\beta-\alpha)}$ and m would be a rotation, (2) distinct elements since $mr^\alpha = mr^\beta \Rightarrow r^\alpha = r^\beta$.

Can another reflection be in the group say $\tilde{m}$? If $\tilde{m} \neq mr^\alpha$, then $m\tilde{m}$ is by definition a rotation in G, that is $m\tilde{m} = r^\alpha$, since we have shown that all rotations of G are in $\langle r(\theta_1)\rangle$. Now this shows that

$$\tilde{m} = m^{-1}r^\alpha = mr^\alpha, \text{ and } (mr^\alpha)(mr^\alpha) = 1 \Rightarrow mr^\alpha m = r^{-\alpha}.$$

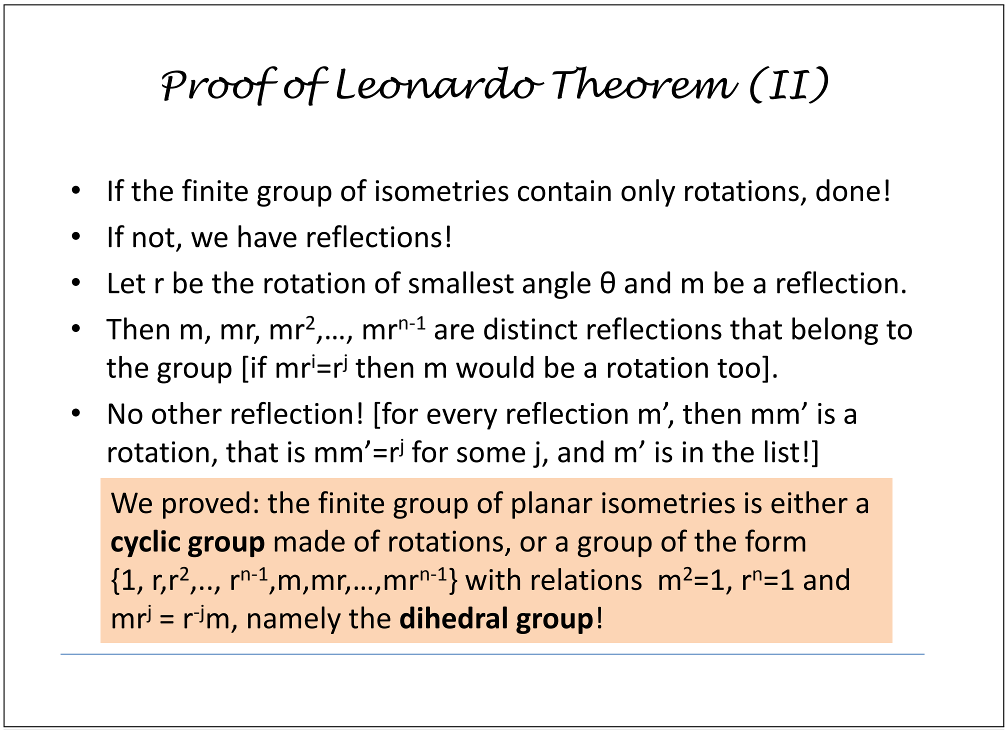
Since $m^2 = 1$ as for any reflection, we proved that

$$G = \{1, r, r^2, \ldots, r^{l-1}, m, mr, \ldots, mr^{l-1}\},\ m^2 = 1,\ r^l = 1, mr^\alpha m = r^{-\alpha}.$$

The group G is therefore recognized as the dihedral group

$$D_p = \{\langle r, m\rangle | m^2 = 1, r^l = 1, mr = r^{-1}m\}.$$

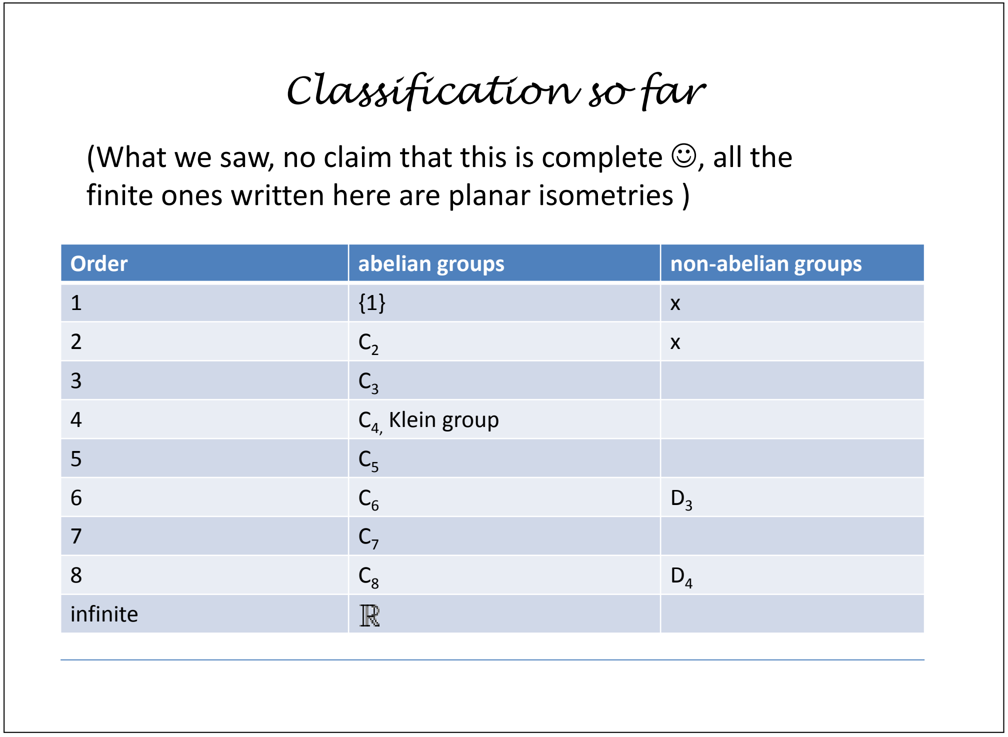
Therefore we proved that a finite group of planar symmetries is either cyclic of some order l or dihedral of order $2l$ for some $l \in \mathbb{N}$. $\square$



Proof of Leonardo Theorem (II)

- If the finite group of isometries contain only rotations, done!
- If not, we have reflections!
- Let r be the rotation of smallest angle θ and m be a reflection.
- Then $m, mr, mr^2, \ldots, mr^{n-1}$ are distinct reflections that belong to the group [if $mr^i=r^j$ then m would be a rotation too].
- No other reflection! [for every reflection m’, then mm’ is a rotation, that is $mm'=r^j$ for some j, and m’ is in the list!]

We proved: the finite group of planar isometries is either a **cyclic group** made of rotations, or a group of the form $\{1, r, r^2, \ldots, r^{n-1}, m, mr, \ldots, mr^{n-1}\}$ with relations $m^2=1$, $r^n=1$ and $mr^j = r^{-j}m$, namely the **dihedral group**!



Classification so far

(What we saw, no claim that this is complete ☺, all the finite ones written here are planar isometries)

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	
4	$C_{4,}$ Klein group	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8	D_4
infinite	$\mathbb{R}$	

Let us look at our table of small groups, up to order 8.

order n	abelian	non-abelian
1	$C_1 \simeq \{1\}$	**x**
2	C_2	**x**
3	C_3	**x**
4	C_4, Klein group	**x**
5	C_5	**x**
6	C_6	D_3
7	C_7	**x**
8	C_8	D_4

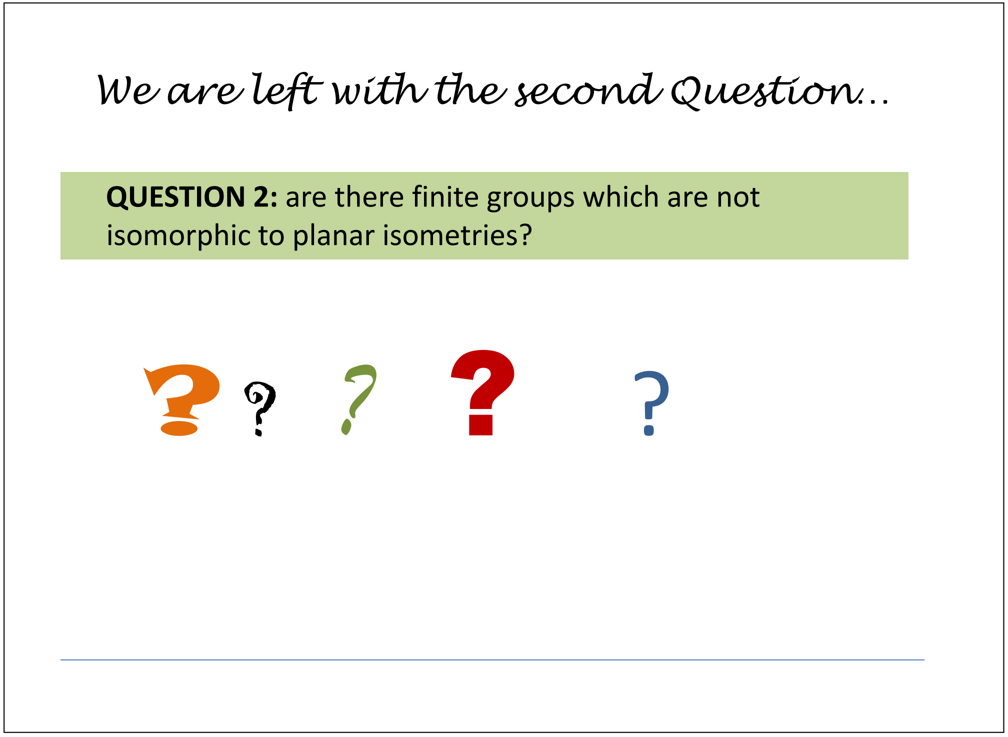
Using Leonardo Theorem, we know that planar isometries only provide cyclic and dihedral groups, so if we want to find potential more groups to add in this table, we cannot rely on planar geometry anymore! This leads to the second question we addressed earlier this chapter:

Are there finite groups which are not isomorphic to subgroups of the group of planar isometries?

Classification so far

Invertible mod 2,3,4,5,6,7 are cyclic, invertible mod 8 are $C_2 x C_2$
[done in Exercises for 5 and 8, same computation for others!]

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	
4	$C_{4,}$ Klein group	
5	C_5	
6	C_6	D_3
7	C_7	
8	C_8	D_4
infinite	$\mathbb{R}$	



We are left with the second Question…

QUESTION 2: are there finite groups which are not isomorphic to planar isometries?

? ? ? ? ?

Exercises for Chapter 6

Exercise 34. Show that any planar isometry of $\mathbb{R}^2$ is a product of at most 3 reflections.

Exercise 35. Look at the pictures on the wiki (available on edventure), and find the symmetry group of the different images shown.

Chapter 7

Permutation Groups

We started the study of groups by considering planar isometries. In the previous chapter, we learnt that finite groups of planar isometries can only be cyclic or dihedral groups. Furthermore, all the groups we have seen so far are, up to isomorphisms, either cyclic or dihedral groups! It is thus natural to wonder whether there are finite groups out there which cannot be interpreted as isometries of the plane. To answer this question, we will study next permutations. Permutations are usually studied as combinatorial objects, we will see in this chapter that they have a natural group structure, and in fact, there is a deep connection between finite groups and permutations!

We know intuitively what is a permutation: we have some objects from a set, and we exchange their positions. However, to work more precisely, we need a formal definition of what is a permutation.

Question 2 after Lagrange Theorem

QUESTION 2: are there finite groups which are not isomorphic to planar isometries (cyclic or dihedral groups)?

Order	abelian groups	non-abelian groups
1	{1}	x
2	C_2	x
3	C_3	x
4	$C_{4,}$ Klein group	x
5	C_5	x
6	C_6	D_3
7	C_7	x
8	C_8	D_4
infinite	$\mathbb{R}$	

What is a Permutation ? (I)

- Intuitively, we know what a permutation is…

http://www.virtualmagie.com/ubbthreads/ubbthreads.php/ubb/download/Number/3018/filename/3415%20net.jpg

Definition 15. A permutation of a set X is a function $\sigma : X \to X$ that is one-to-one and onto, i.e., a bijective map.

Let us make a small example to understand better the connection between the intuition and the formal definition.

Example 25. Consider a set X containing 3 objects, say a triangle, a circle and a square. A permutation of $X = \{\triangle, \circ, \square\}$ might send for example

$$\triangle \mapsto \triangle, \ \circ \mapsto \square, \ \square \mapsto \circ,$$

and we observe that what just did is exactly to define a bijection on the set X, namely a map $\sigma : X \to X$ defined as

$$\sigma(\triangle) = \triangle, \ \sigma(\circ) = \square, \ \sigma(\square) = \circ.$$

Since what matters for a permutation is how many objects we have and not the nature of the objects, we can always consider a permutation on a set of n objects where we label the objects by $\{1, \ldots, n\}$. The permutation of Example 25 can then be rewritten as $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ such that

$$\sigma(1) = 1, \ \sigma(2) = 3, \ \sigma(3) = 2, \text{ or } \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Permutation maps, being bijective, have inverses and the maps combine naturally under composition of maps, which is associative. There is a natural identity permutation $\sigma : X \to X$, $X = \{1, 2, 3, \ldots, n\}$ which is

$$\sigma(k) \mapsto k.$$

Therefore all the permutations of a set $X = \{1, 2, \ldots, n\}$ form a group under composition. This group is called the symmetric group S_n of degree n.

What is the order of S_n? Let us count how many permutations of $\{1, 2, \ldots, n\}$ we have. We have to fill the boxes

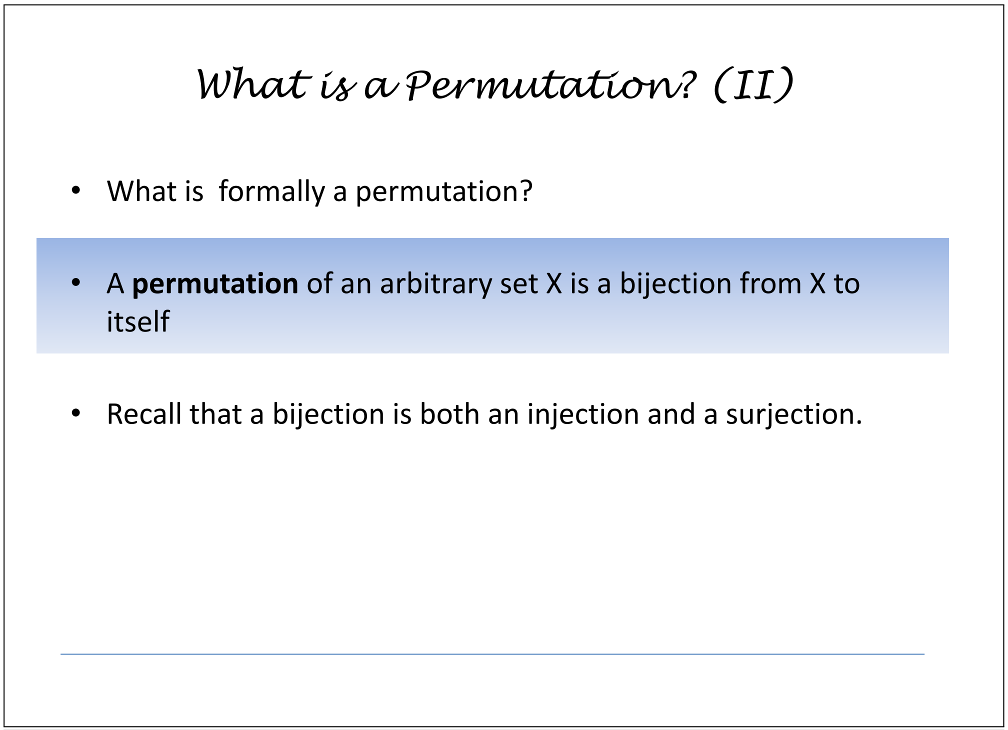
$$\begin{array}{|c|c|c|c|c|}\hline & & & \cdots & \\ \hline \multicolumn{1}{c}{1} & \multicolumn{1}{c}{2} & \multicolumn{1}{c}{3} & \multicolumn{1}{c}{\cdots} & \multicolumn{1}{c}{n} \end{array}$$

with numbers $\{1, 2, \ldots, n\}$ with no repetitions. For box 1, we have n possible candidates. Once one number has been used, for box 2, we have $(n-1)$ candidates, ... Therefore we have

$$n(n-1)(n-2)\cdots 1 = n!$$

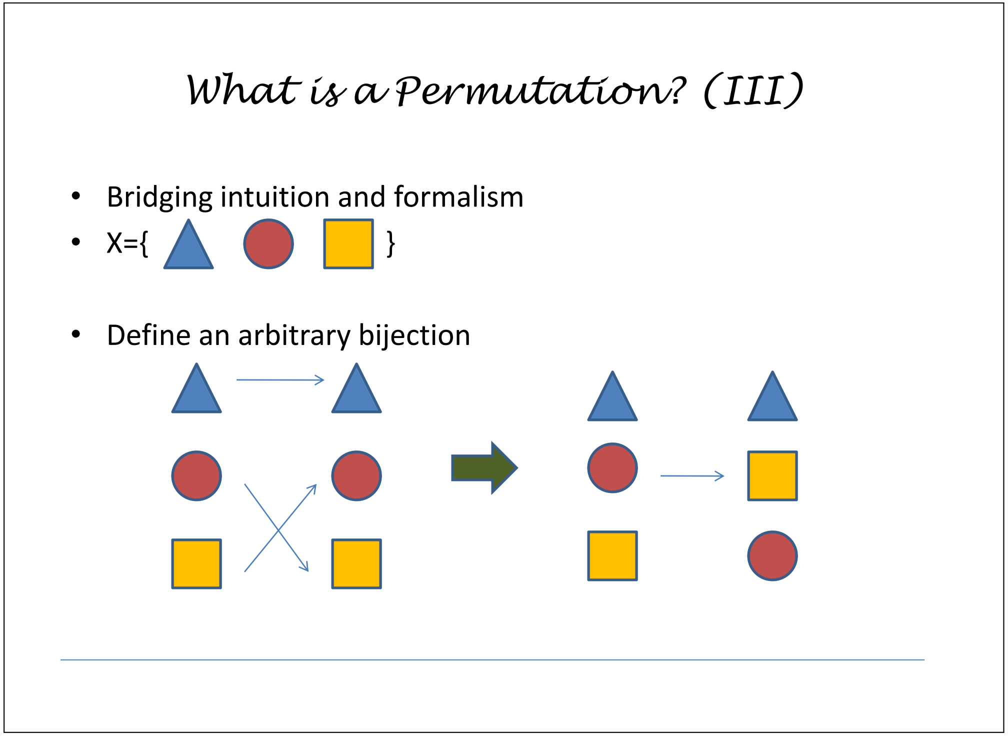
permutations and the order of S_n is

$$|S_n| = n!.$$



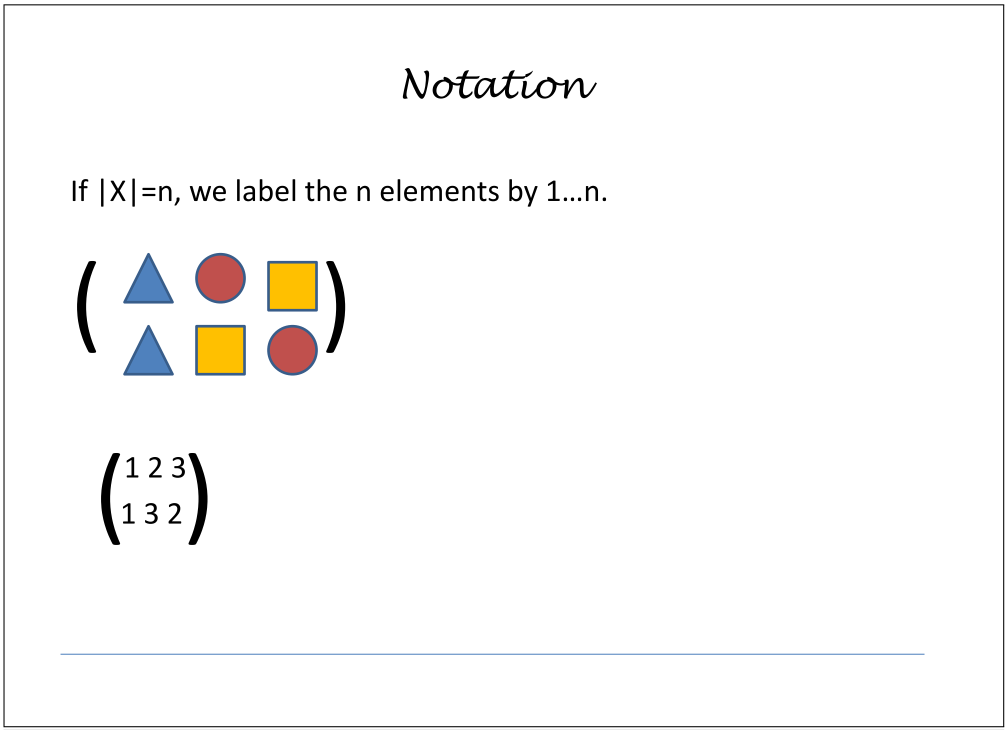
What is a Permutation? (II)

- What is formally a permutation?
- A **permutation** of an arbitrary set X is a bijection from X to itself
- Recall that a bijection is both an injection and a surjection.



What is a Permutation? (III)

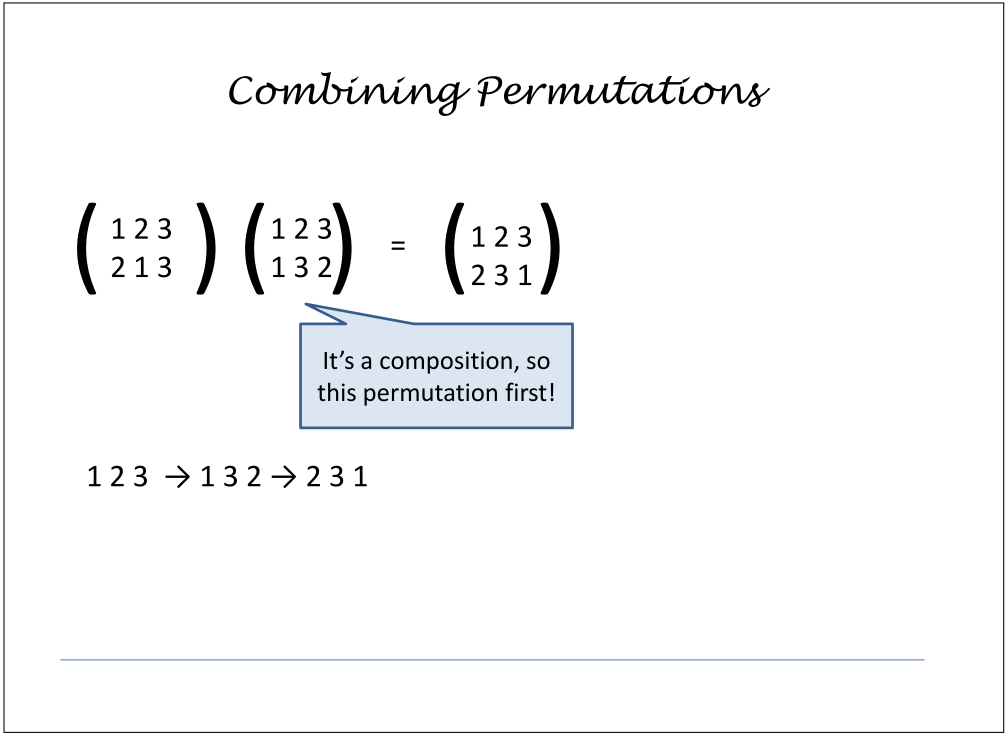
- Bridging intuition and formalism
- X={ ▲ ● ■ }
- Define an arbitrary bijection



Notation

If |X|=n, we label the n elements by 1…n.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



Combining Permutations

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

It's a composition, so this permutation first!

1 2 3 → 1 3 2 → 2 3 1

Group Structure of Permutations (I)

- All permutations of a set X of n elements form a group under composition, called the **symmetric group** on n elements, denoted by S_n.

Composition of two bijections is a bijection

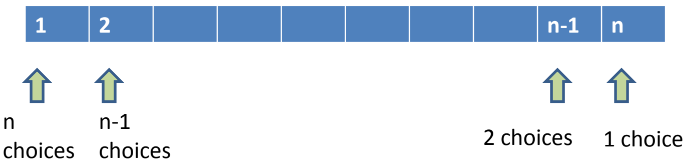
- Identity = do-nothing (do no permutation)
- Every permutation has an inverse, the inverse permutation.

A permutation is a bijection!

- Non abelian (the two permutations of the previous slide do not commute for example!)

Group Structure of Permutations (II)

The order of the group S_n of permutations on a set X of elements is n!



$|S_n| = n!$

Let us see a few examples of symmetric groups S_n.

Example 26. If $n = 1$, S_1 contains only one element, the permutation identity!

Example 27. If $n = 2$, then $X = \{1, 2\}$, and we have only two permutations:

$$\sigma_1 : 1 \mapsto 1,\ 2 \mapsto 2$$

and

$$\sigma_2 : 1 \mapsto 2,\ 2 \mapsto 1,$$

and $S_2 = \{\sigma_1, \sigma_2\}$. The Cayley table of S_2 is

	σ_1	σ_2
σ_1	σ_1	σ_2
σ_2	σ_2	σ_1

.

Let us introduce the *cycle notation*. We write (12) to mean that 1 is sent to 2, and 2 is sent to 1. With this notation, we write

$$S_2 = \{(), (12)\}\,.$$

This group is isomorphic to C_2, and it is abelian.

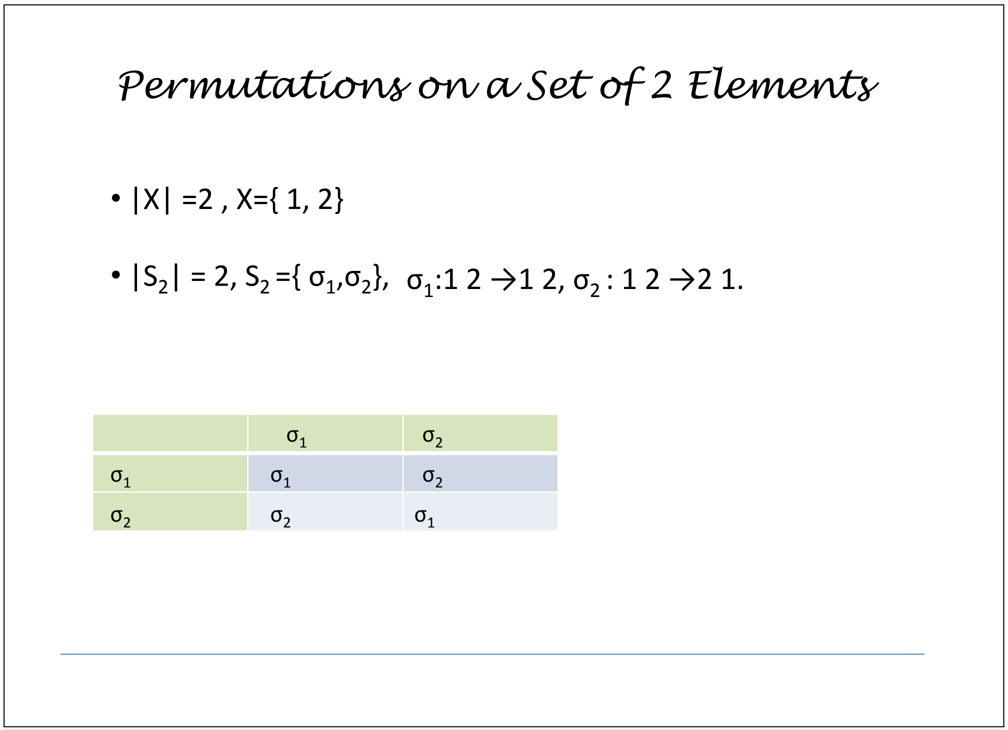
The permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

of Example 25 in the cycle notation is written as (23). We can combine two such permutations:

$$(12)(23)$$

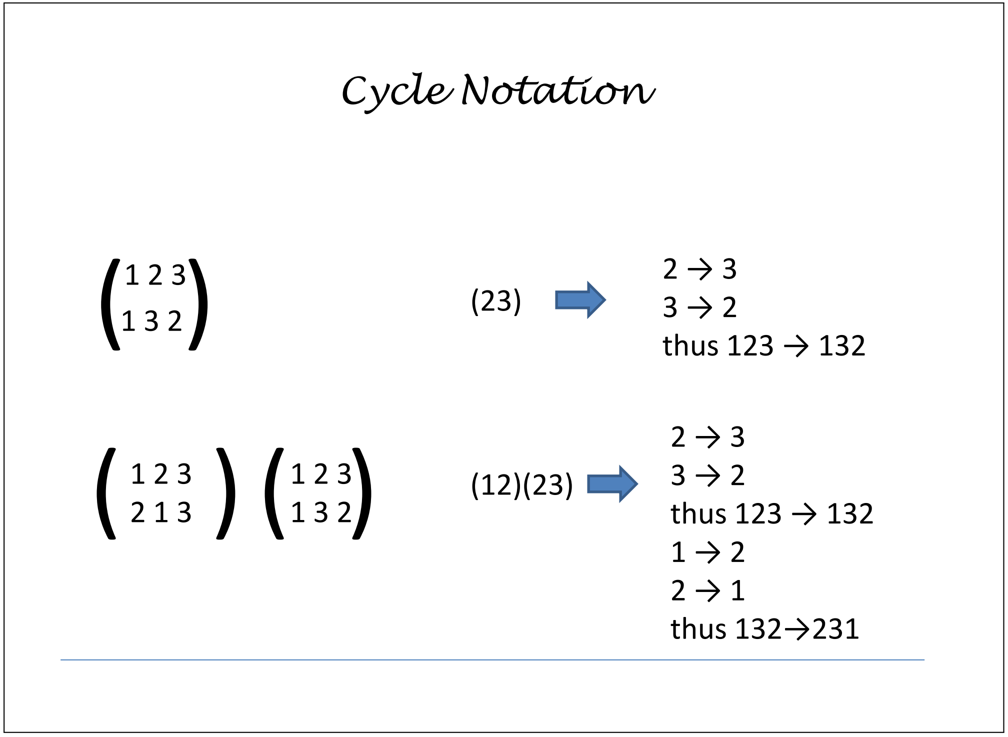
which means that we first permute 2 and 3: 1 2 3 $\mapsto$ 1 3 2 and then we permute 1 and 2: 1 3 2 $\mapsto$ 2 3 1. Let us look next at the group S_3.



Permutations on a Set of 2 Elements

- $|X| = 2$, $X = \{1, 2\}$
- $|S_2| = 2$, $S_2 = \{\sigma_1, \sigma_2\}$, $\sigma_1: 1\ 2 \to 1\ 2$, $\sigma_2: 1\ 2 \to 2\ 1$.

	σ_1	σ_2
σ_1	σ_1	σ_2
σ_2	σ_2	σ_1



Cycle Notation

$\begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}$ $(23) \Rightarrow$

2 → 3
3 → 2
thus 123 → 132

$\begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix} \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}$ $(12)(23) \Rightarrow$

2 → 3
3 → 2
thus 123 → 132
1 → 2
2 → 1
thus 132→231

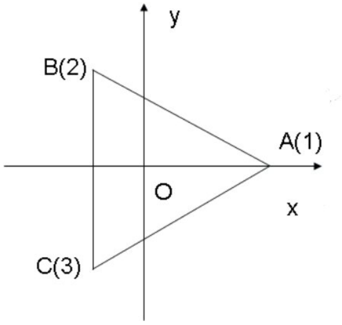
Example 28. If $n = 3$, we consider the set $X = \{1, 2, 3\}$. Since $3! = 6$, we have 6 permutations:

$$S_3 = \{\sigma_1 = (), \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132)\}.$$

We compute the Cayley table of S_3.

	()	(12)	(23)	(13)	(123)	(132)
()	()	(12)	(23)	(13)	(123)	(132)
(12)	(12)	()	(123)	(132)	(23)	(13)
(23)	(23)	(132)	()	(123)	(13)	(12)
(13)	(13)	(123)	(132)	()	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	()
(132)	(132)	(23)	(13)	(12)	()	(123)

We see from the Cayley table that S_3 is indeed isomorphic to D_3! This can also be seen geometrically as follows. Consider an equilateral triangle, and label its 3 vertices by A, B, C, and label the locations of the plane where each is by 1,2,3 (thus vertex A is at location 1, vertex B at location 2 and vertex C as location 3). Let us now rotate the triangle by r (120 degrees counterclockwise), to find that now, at position 1 we have C, at position 2 we have A and at position 3 we have B, and we apply all the symmetries of the triangle, and see which vertex is sent to position 1,2, and 3 respectively:



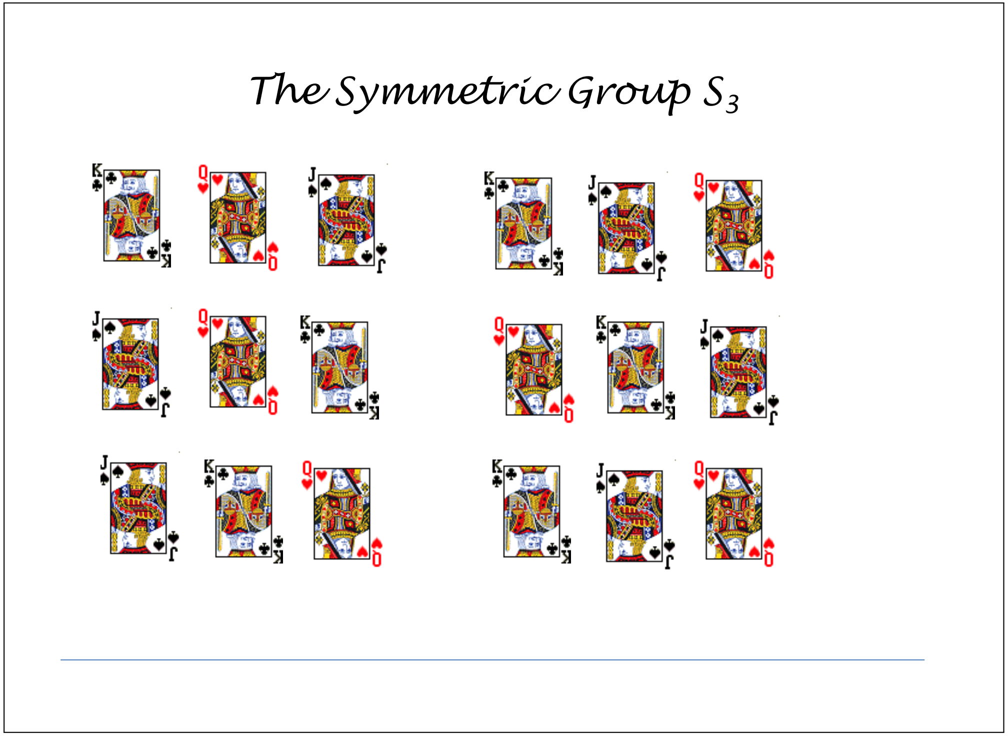
	1	2	3	
1	A	B	C	()
r	C	A	B	(213)
r^2	B	C	A	(123)
m	A	C	B	(23)
rm	B	A	C	(12)
r^2m	C	B	A	(13)

and we see that to each symmetry corresponds a permutation. For example, r sends ABC to CAB and thus we have (132).

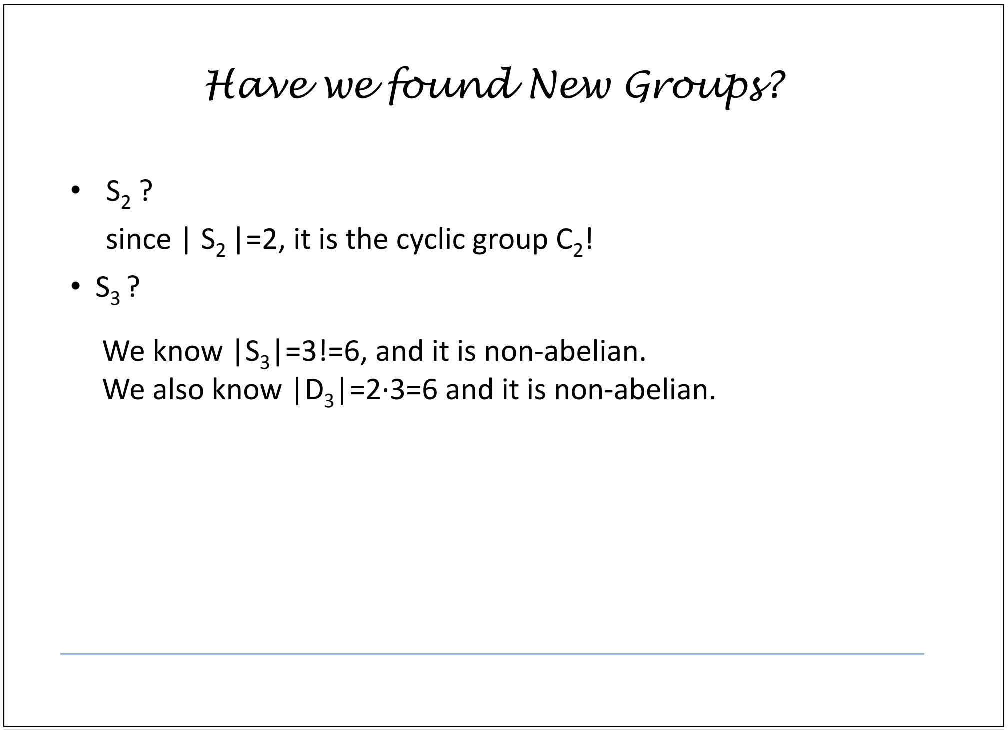
Permutations on a Set of 3 Elements

- |X|=3, X={1 2 3}
- σ_1 :123 → 123 (), σ_2 :123 → 213 (12) ,σ_3 :123→321 (13) , σ_4 :123 → 132 (23) , σ_5: 123→231 (123) , σ_6 : 123→312 (132) .

	()	(1,2)	(2,3)	(1,3)	(1,2,3)	(1,3,2)
()	()	(1,2)	(2,3)	(1,3)	(1,2,3)	(1,3,2)
(1,2)	(1,2)	()	(1,2,3)	(1,3,2)	(2,3)	(1,3)
(2,3)	(2,3)	(1,3,2)	()	(1,2,3)	(1,3)	(1,2)
(1,3)	(1,3)	(1,2,3)	(1,3,2)	()	(1,2)	(2,3)
(1,2,3)	(1,2,3)	(1,3)	(1,2)	(2,3)	(1,3,2)	()
(1,3,2)	(1,3,2)	(2,3)	(1,3)	(1,2)	()	(1,2,3)



The Symmetric Group S_3

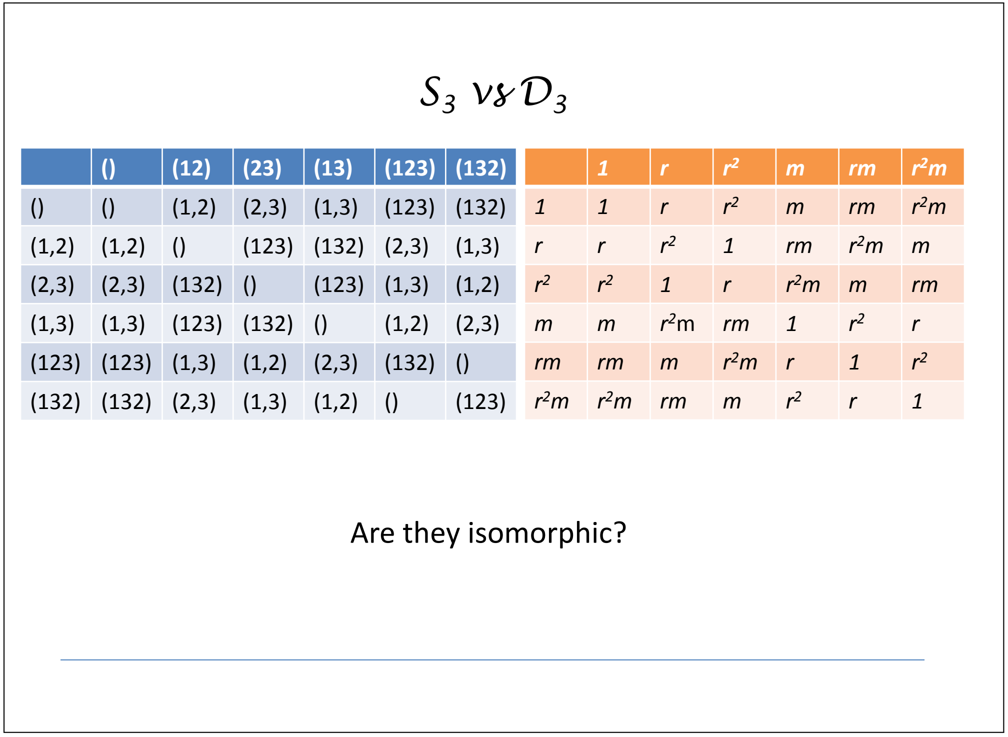


Have we found New Groups?

- S_2 ?

  since | S_2 |=2, it is the cyclic group C_2!
- S_3 ?

  We know |S_3|=3!=6, and it is non-abelian.
  We also know |D_3|=2·3=6 and it is non-abelian.

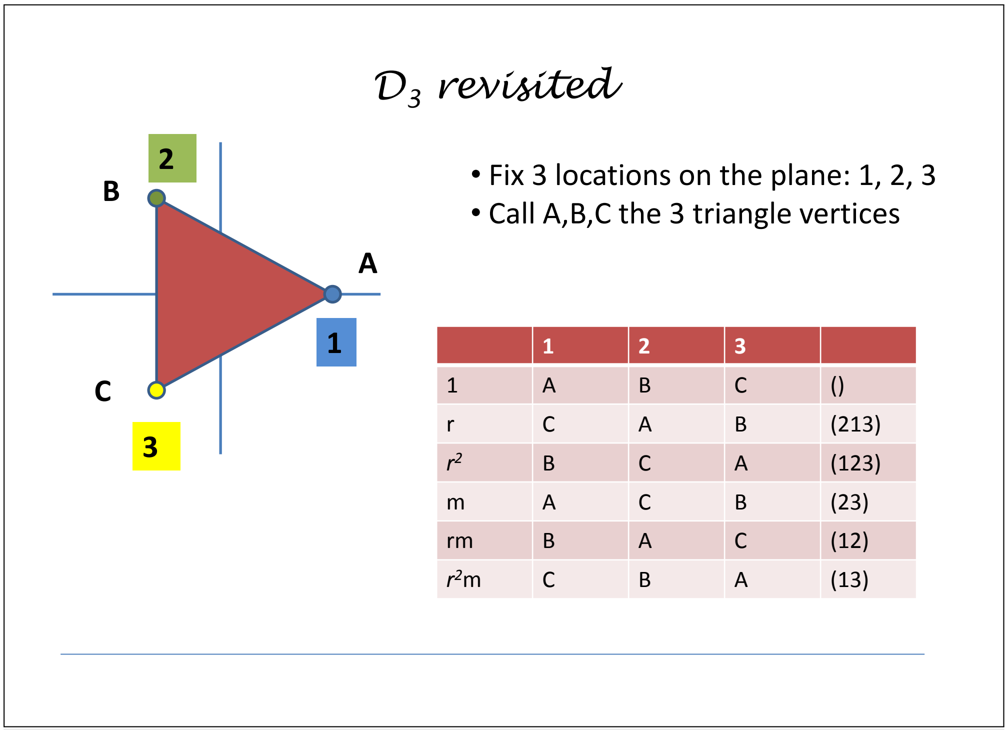


S_3 vs D_3

	()	(12)	(23)	(13)	(123)	(132)
()	()	(1,2)	(2,3)	(1,3)	(123)	(132)
(1,2)	(1,2)	()	(123)	(132)	(2,3)	(1,3)
(2,3)	(2,3)	(132)	()	(123)	(1,3)	(1,2)
(1,3)	(1,3)	(123)	(132)	()	(1,2)	(2,3)
(123)	(123)	(1,3)	(1,2)	(2,3)	(132)	()
(132)	(132)	(2,3)	(1,3)	(1,2)	()	(123)

	1	r	r^2	m	rm	r^2m
1	1	r	r^2	m	rm	r^2m
r	r	r^2	1	rm	r^2m	m
r^2	r^2	1	r	r^2m	m	rm
m	m	r^2m	rm	1	r^2	r
rm	rm	m	r^2m	r	1	r^2
r^2m	r^2m	rm	m	r^2	r	1

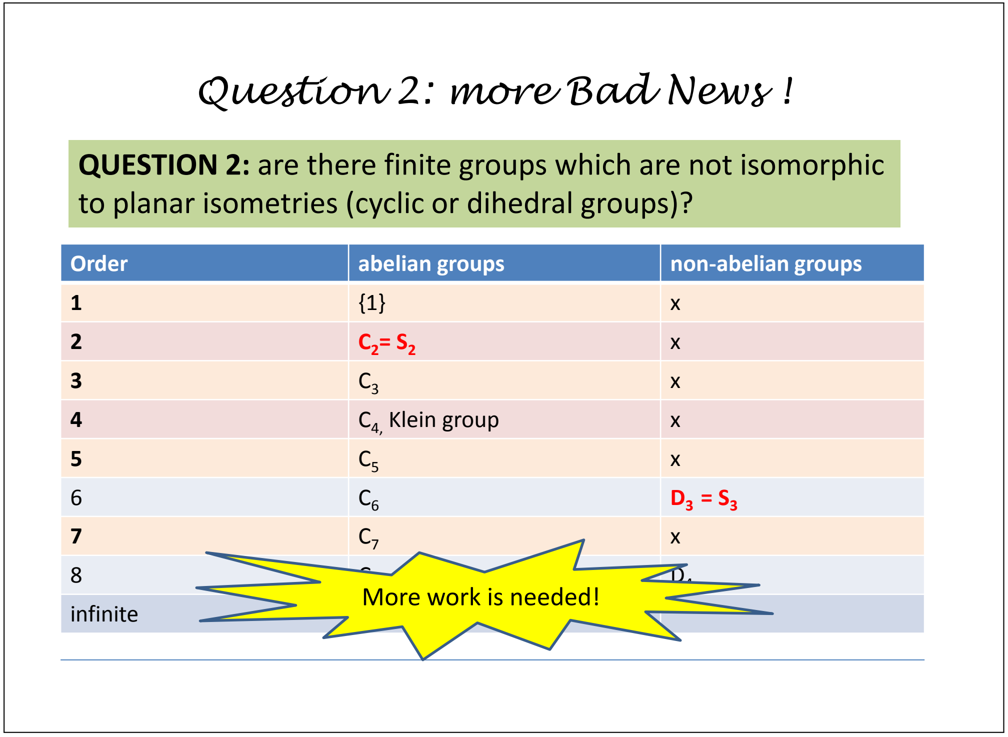
Are they isomorphic?



D_3 revisited

- Fix 3 locations on the plane: 1, 2, 3
- Call A,B,C the 3 triangle vertices

	1	**2**	**3**	
1	A	B	C	()
r	C	A	B	(213)
r^2	B	C	A	(123)
m	A	C	B	(23)
rm	B	A	C	(12)
r^2m	C	B	A	(13)



Question 2: more Bad News !

QUESTION 2: are there finite groups which are not isomorphic to planar isometries (cyclic or dihedral groups)?

Order	**abelian groups**	**non-abelian groups**
1	{1}	x
2	**$C_2 = S_2$**	x
3	C_3	x
4	$C_{4,}$ Klein group	x
5	C_5	x
6	C_6	**$D_3 = S_3$**
7	C_7	x
8	[illegible]	D_4
infinite		

More work is needed!

Thus despite the introduction of a new type of groups, the groups of permutations, we still have not found a finite group which is not a cyclic or a dihedral group. We need more work! For that, we start by noting that permutations can be described in terms of matrices.

Any permutation σ of the elements $\{1,2,\dots,n\}$ can be described by

$$\begin{bmatrix} \sigma(1) \\ \sigma(2) \\ \vdots \\ \sigma(n) \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 1 & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 1 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ \vdots \\ n \end{bmatrix} = \underbrace{\begin{bmatrix} e^T_{\sigma(1)} \\ \vdots \\ e^T_{\sigma(n)} \end{bmatrix}}_{P_\sigma} \begin{bmatrix} 1 \\ \vdots \\ n \end{bmatrix},$$

where the kth row of the binary matrix is given by $e^T_{\sigma(k)} = (0,\dots,0,1,0,\dots,0)$, where 1 is at location $\sigma(k)$. Now $e_1,\dots,e_n$ are a set of orthogonal vectors, that is, satisfying

$$e_k^T e_s = \langle e_k, e_s \rangle = \delta_{ks} = \begin{cases} 0 & if\ k \neq s \\ 1 & if\ k = s \end{cases}, \tag{7.1}$$

which form a standard basis of $\mathbb{R}^n$. Let us derive some properties of the matrix P_σ.

Property 1. The matrix P_σ is orthogonal, that is $P_\sigma P_\sigma^T = I_n$, where I_n is the identity matrix. This follows from

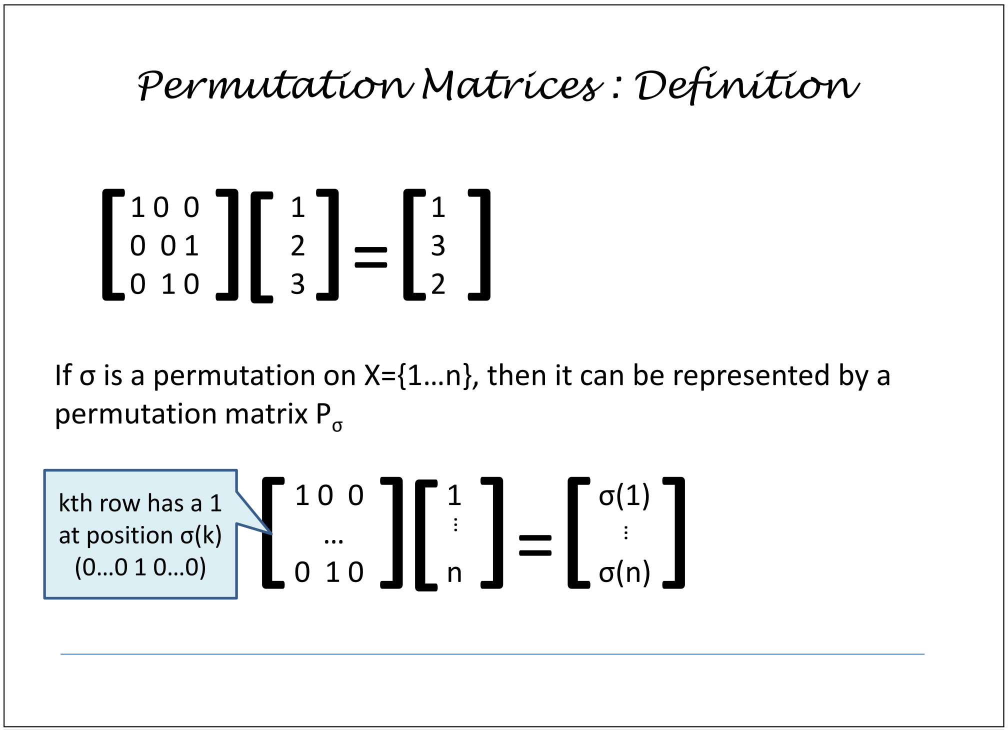
$$\begin{bmatrix} e^T_{\sigma(1)} \\ e^T_{\sigma(2)} \\ \vdots \\ e^T_{\sigma(n)} \end{bmatrix} \begin{bmatrix} e^T_{\sigma(1)} & e^T_{\sigma(2)} & \cdots & e^T_{\sigma(n)} \end{bmatrix} = \begin{bmatrix} & \vdots & \\ \cdots & \langle e_{\sigma(i)}, e_{\sigma(j)} \rangle & \cdots \\ & \vdots & \end{bmatrix} = I_n$$

using (7.1). Hence the inverse of a permutation matrix is its transpose.

Property 2. Using that $\det(AB) = \det(A)\det(B)$ and $\det(A^T) = \det(A)$, we get

$$\det(P_\sigma P_\sigma^T) = \det(I) = 1.$$

Therefore $\det(P_\sigma) = \pm 1$. $(\det(P_\sigma^T) = \det(P_\sigma) \Rightarrow (\det P_\sigma)^2 = 1)$.



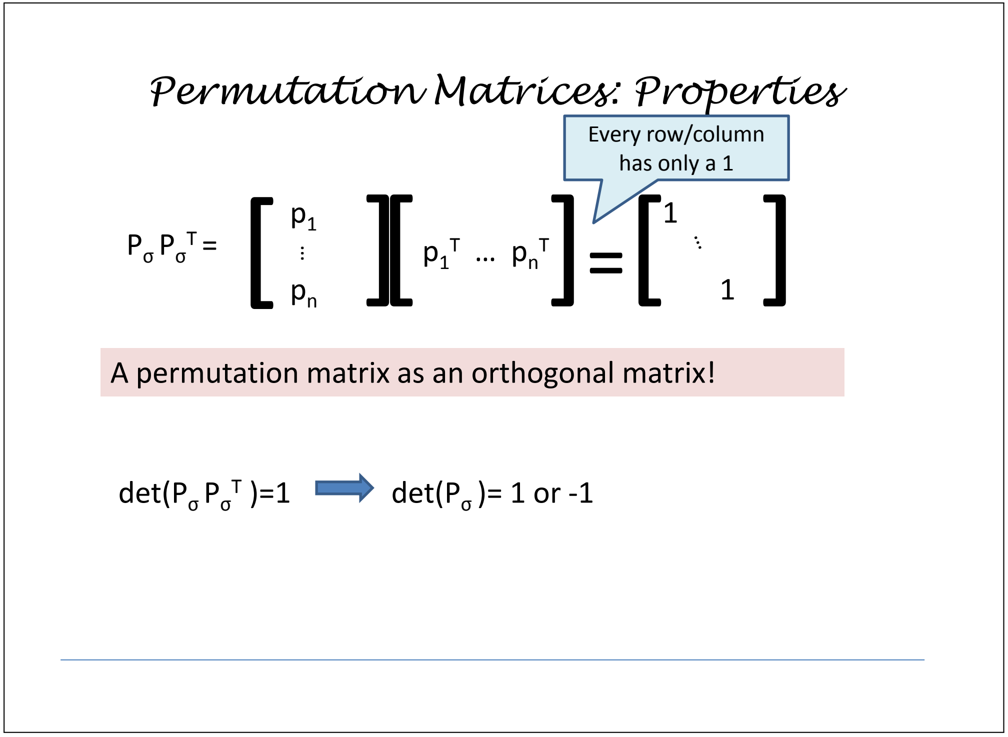
Permutation Matrices : Definition

$$\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\3\\2\end{bmatrix}$$

If σ is a permutation on X={1…n}, then it can be represented by a permutation matrix P_σ

kth row has a 1 at position σ(k) (0…0 1 0…0)

$$\begin{bmatrix}1\ 0\ 0\\ \cdots\\ 0\ 1\ 0\end{bmatrix}\begin{bmatrix}1\\ \vdots\\ n\end{bmatrix}=\begin{bmatrix}\sigma(1)\\ \vdots\\ \sigma(n)\end{bmatrix}$$



Permutation Matrices: Properties

Every row/column has only a 1

$$P_\sigma P_\sigma^T = \begin{bmatrix}p_1\\ \vdots\\ p_n\end{bmatrix}\begin{bmatrix}p_1^T & \dots & p_n^T\end{bmatrix}=\begin{bmatrix}1 & & \\ & \ddots & \\ & & 1\end{bmatrix}$$

A permutation matrix as an orthogonal matrix!

$\det(P_\sigma P_\sigma^T)=1$ ➡ $\det(P_\sigma)= 1$ or -1

Property 3. We will show next that any permutation can be decomposed as a chain of “elementary” permutations called transpositions, or exchanges.

We consider the permutation σ given by

$$\begin{bmatrix} \sigma(1) \\ \vdots \\ \sigma(n) \end{bmatrix} = \begin{bmatrix} e^T_{\sigma(1)} \\ \vdots \\ e^T_{\sigma(n)} \end{bmatrix} \begin{bmatrix} 1 \\ \vdots \\ n \end{bmatrix}.$$

We shall produce σ from $(1, 2, \ldots, n)$ by successively moving $\sigma(1)$ to the first place and 1 to the place of $\sigma(1)$, then $\sigma(2)$ to the second place and whoever is in the second place after the first exchange to the place of $\sigma(2)$ place, etc..

After moving $\sigma(1)$ to the first place, using a matrix P, we get

$$\begin{bmatrix} \sigma(1) \\ 2 \\ \vdots \\ 1 \\ \vdots \\ n \end{bmatrix} = P_{n\times n} \begin{bmatrix} 1 \\ 2 \\ \vdots \\ \sigma(1) \\ \vdots \\ n \end{bmatrix}.$$

After this step, we use an $(n-1) \times (n-1)$ permutation matrix to bring $\sigma(2)$ to the second place as follows (without affecting $\sigma(1)$):

$$\begin{bmatrix} \sigma(1) \\ \sigma(2) \\ \vdots \\ 2 \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & P_{(n-1)\times(n-1)} \end{bmatrix} \begin{bmatrix} \sigma(1) \\ 2 \\ \vdots \\ \sigma(2) \\ \vdots \\ n \end{bmatrix},$$

and so on. From this process, it is clear that at every stage we have either a matrix of exchange in which two rows of the identity are exchanged, or if the output happens to have the next value in its designated place an identity matrix. The process will necessarily terminate after n steps and will yield the permutation σ as desired.

Transpositions

A **transposition** (exchange) is a permutation that swaps two elements and does not change the others.

- In cycle notation, a transposition has the form (i j).

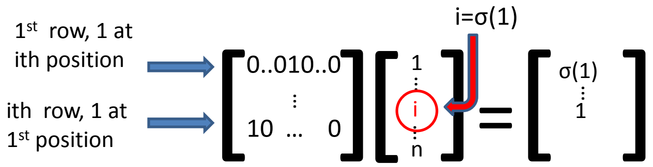
Example: (1 2) on the set X={1,2,3,4} means 1234 →2134.

- In matrix notation, a transposition is an identity matrix, but for for two rows that are swapped.

$$\begin{bmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{bmatrix}$$

Decomposition in Transpositions (I)

Any permutation can be decomposed as a product of transpositions.


1^{st} row, 1 at ith position
ith row, 1 at 1^{st} position
i=σ(1)

$$\begin{bmatrix} 0..010..0 \\ \vdots \\ 10 \;\dots\; 0 \end{bmatrix}\begin{bmatrix} 1 \\ \vdots \\ i \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} \sigma(1) \\ \vdots \\ 1 \end{bmatrix}$$

Place similarly σ(2) at the 2nd position, σ(3) at the 3^{rd} position etc, this process stops at most after n steps! (since at every step, either two rows are exchanged, or we have an identity matrix if nothing needs to be changed).

Hence we will be able to write

$$\begin{bmatrix} \sigma(1) \\ \sigma(2) \\ \vdots \\ \sigma(n) \end{bmatrix} = E_n E_{n-1} \cdots E_2 E_1 \begin{bmatrix} 1 \\ 2 \\ \vdots \\ n \end{bmatrix}$$

where $E_i = \begin{cases} \text{either an elementary exchange matrix of size n} \times \text{n} \\ \text{or an identity matrix of size n} \times \text{n} \end{cases}.$
Now, we know from the property of the determinant that exchanging two rows in a matrix induces a sign change in the determinant. Hence we have

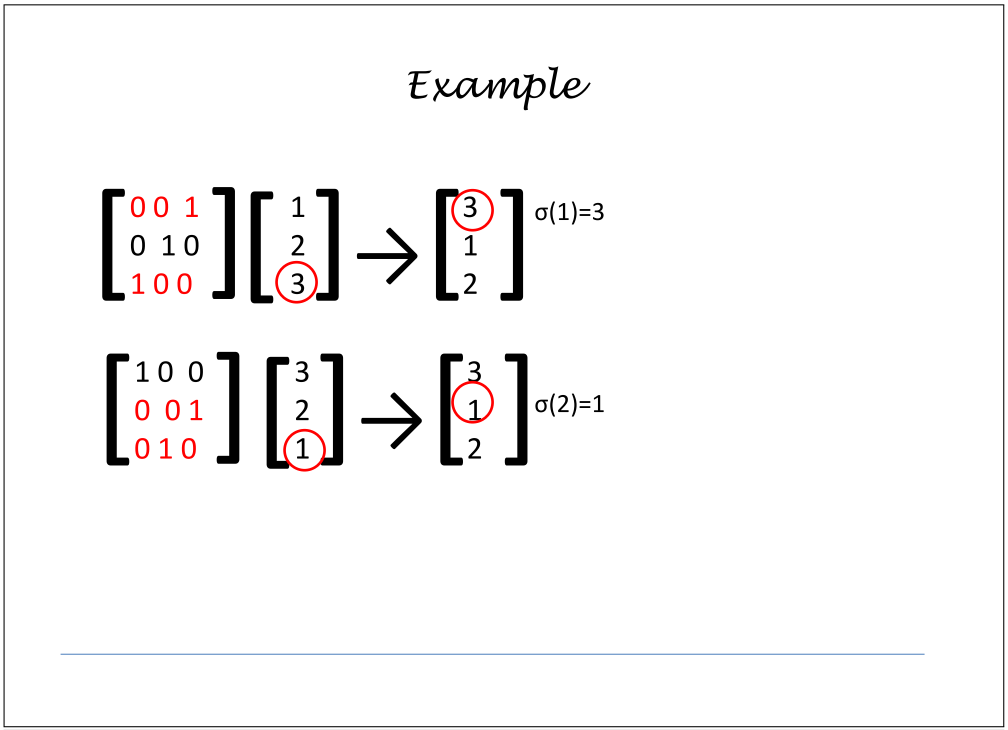
$$\det E_i = \begin{cases} -1 & \text{if it is a proper exchange} \\ 1 & \text{if it is } I_{n \times n} \end{cases}.$$

Therefore we have shown that for any permutation, we have a decomposition into a sequence of transpositions (or exchanges), and we need at most n of them to obtain any permutation. Hence for any σ we have:

$$P_\sigma = E_n E_{n-1} \cdots E_1$$

and

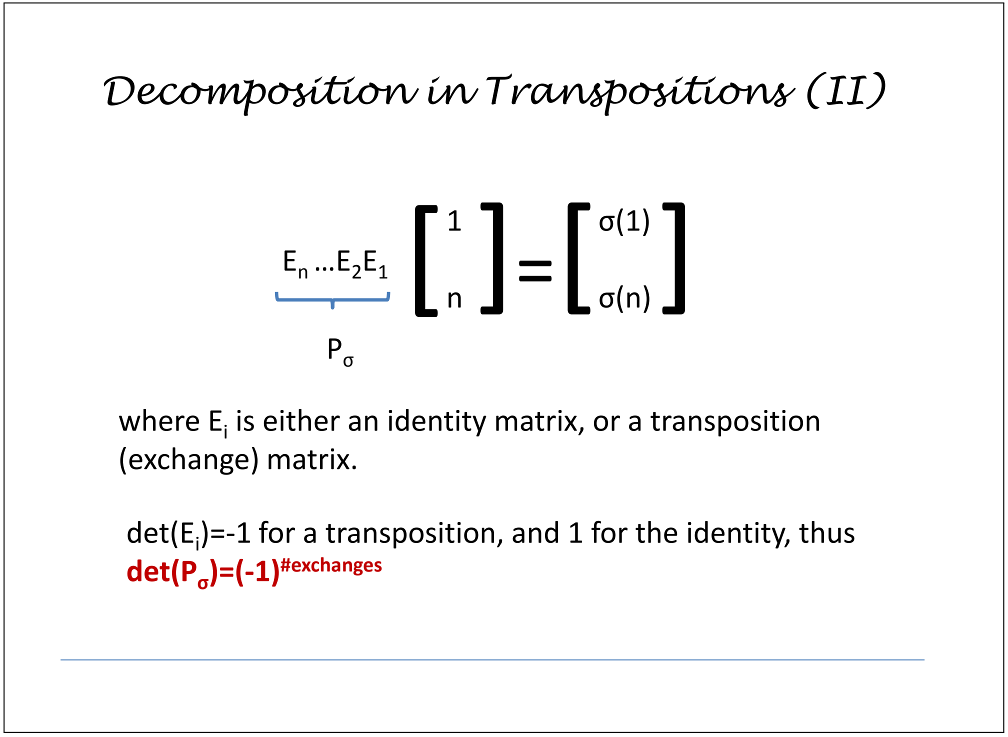
$$\det P_\sigma = \det E_n \det E_{n-1} \cdots \det E_1 = (-1)^{\#\text{ of exchanges}}.$$



Example

$$\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}\begin{bmatrix}1\\2\\\textcircled{3}\end{bmatrix}\rightarrow\begin{bmatrix}\textcircled{3}\\1\\2\end{bmatrix}\quad \sigma(1)=3$$

$$\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\begin{bmatrix}3\\2\\\textcircled{1}\end{bmatrix}\rightarrow\begin{bmatrix}3\\\textcircled{1}\\2\end{bmatrix}\quad \sigma(2)=1$$



Decomposition in Transpositions (II)

$$\underbrace{E_n \ldots E_2 E_1}_{P_\sigma}\begin{bmatrix}1\\ \\ n\end{bmatrix}=\begin{bmatrix}\sigma(1)\\ \\ \sigma(n)\end{bmatrix}$$

where E_i is either an identity matrix, or a transposition (exchange) matrix.

$\det(E_i)=-1$ for a transposition, and 1 for the identity, thus **$\det(P_\sigma)=(-1)^{\#\text{exchanges}}$**

The above development enable us to define the permutation to be even if

$$\det P_\sigma = 1,$$

and odd if

$$\det P_\sigma = -1.$$

Definition 16. The sign/signature of a permutation σ is the determinant of P_σ. It is either 1 if the permutation is even or -1 otherwise.

We have a natural way to combine permutations as bijective maps. In matrix form, we have that if

$$P_{\sigma_A}\begin{bmatrix} 1 \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} \sigma_A(1) \\ \vdots \\ \sigma_A(n) \end{bmatrix}, P_{\sigma_B}\begin{bmatrix} 1 \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} \sigma_B(1) \\ \vdots \\ \sigma_B(n) \end{bmatrix}$$

then

$$P_{\sigma_A}P_{\sigma_B} = P_{\sigma_B \circ \sigma_A}.$$

The description of a permutation via transposition is not unique but the parity is an invariant. We also have that

$$\begin{aligned} sign(\sigma_A \circ \sigma_B) &= sign(\sigma_A)sign(\sigma_B) \\ \det(P_{\sigma_B}P_{\sigma_A}) &= \det(P_{\sigma_B})\det(P_{\sigma_A}). \end{aligned}$$

Then we have the multiplication rule.

	even	odd
even	even	odd
odd	odd	even

This shows the following.

Theorem 14. *All even permutations form a subgroup of permutations.*

Proof. Clearly the identity matrix is an even permutation, since its determinant is 1.

Product of even permutations is even, thus closure is satisfied.

The inverse of an even permutation must be even. To show this, we know

$$P_\sigma^T P_\sigma = I,$$

so $\det(P_\sigma^T) = \det(P_\sigma) \Rightarrow \det(P_\sigma^T) = 1$ if $\det(P_\sigma) = 1$. □

Definition 17. The subgroup A_n of even permutations of the symmetric group S_n is called the alternating group.

Parity of a Permutation

A permutation is **even** if $\det(P_\sigma)=1$ and **odd** if $\det(P_\sigma)=-1$.
The sign/signature of a permutation σ is $\text{sign}(\sigma)=\det(P_\sigma)$.

Example

(132) : 123 →312
123 → 312 thus (13) : 123 →321
321→312 thus (12)(13) : 123 →321→312

$\text{sign}(132)=(-1)^2=1.$

Same result from the matrix approach!

The decomposition in transpositions is far from unique! It is the signature which is unique!!

The Alternating Group

The subset of S_n formed by even permutations is a group, called the **alternating group** A_n.

- The identity is the do-nothing permutation σ= (), its permutation matrix is the identity, and its determinant is 1 and sign(())=1, that is () is even.
- The composition of two even permutations is even, since $\det(P_{\sigma1}P_{\sigma2})= \det(P_{\sigma1}) \det(P_{\sigma2})=1\cdot1=1$.
- If σ is a permutation with matrix P_σ, then its inverse permutation has matrix P_σ^T . Now $\det(P_\sigma P_\sigma^T)=1$ and since $\det(P_\sigma)=1$, we must have $\det(P_\sigma^T)=1$!

Example 29. When $n = 3$, we consider the symmetric group S_3, and identify those permutations which are even. Among the 6 permutations of S_3, 3 are odd and 3 are even. Thus A_3 is isomorphic to the cyclic group C_3 of order 3.

An interesting immediate fact is that the size of the subgroup of even permutations is $\frac{1}{2}n!$, since for every even permutation, one can uniquely associate an odd one by exchanging the first two elements!

Let us go back once more to our original question. We are looking for a group which is not isomorphic to a group of finite planar isometries. Since A_3 is isomorphic to a cyclic group, let us consider the next example, namely A_4.

Since $4! = 24$, we know that $|A_4| = 12$. There is a dihedral group D_6 which also has order 12. Are the two groups isomorphic?

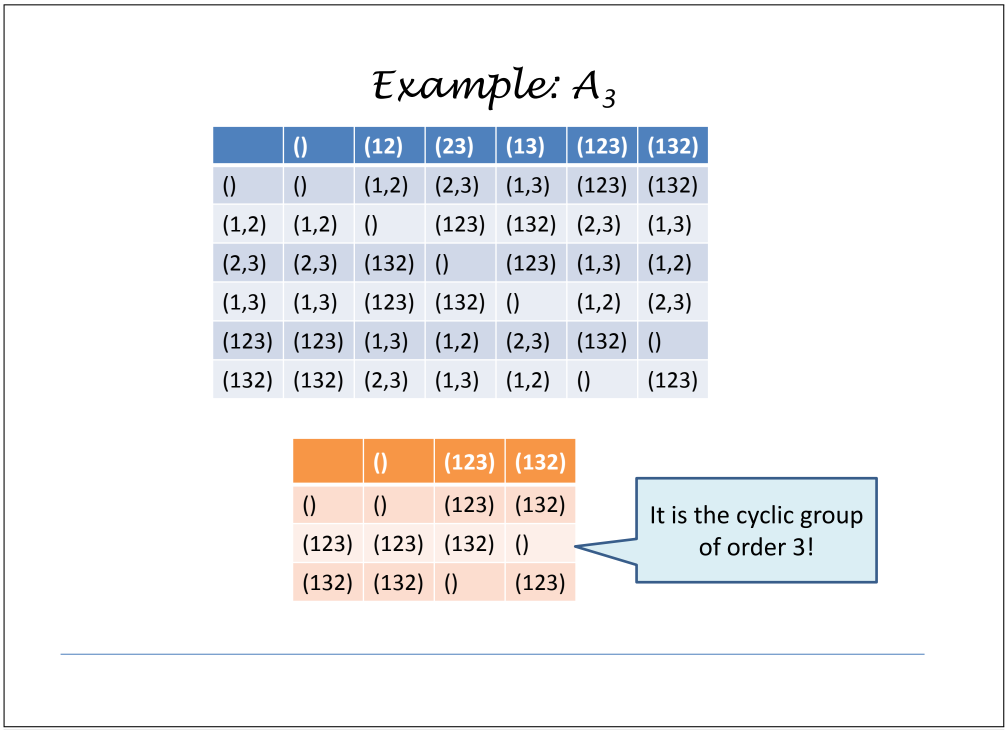
Lagrange theorem tells us that elements of A_4 have an order which divides 12, so it could be 1,2,3,4 or 12. We can compute that there are exactly 3 elements of order 2:

$$(12)(34),\ (13)(24),\ (14)(23),$$

and 8 elements of order 3:

$$(123),\ (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243).$$

This shows that A_4 and D_6 cannot be isomorphic! We thus just found our first example, to show that there is more than cyclic and dihedral groups!

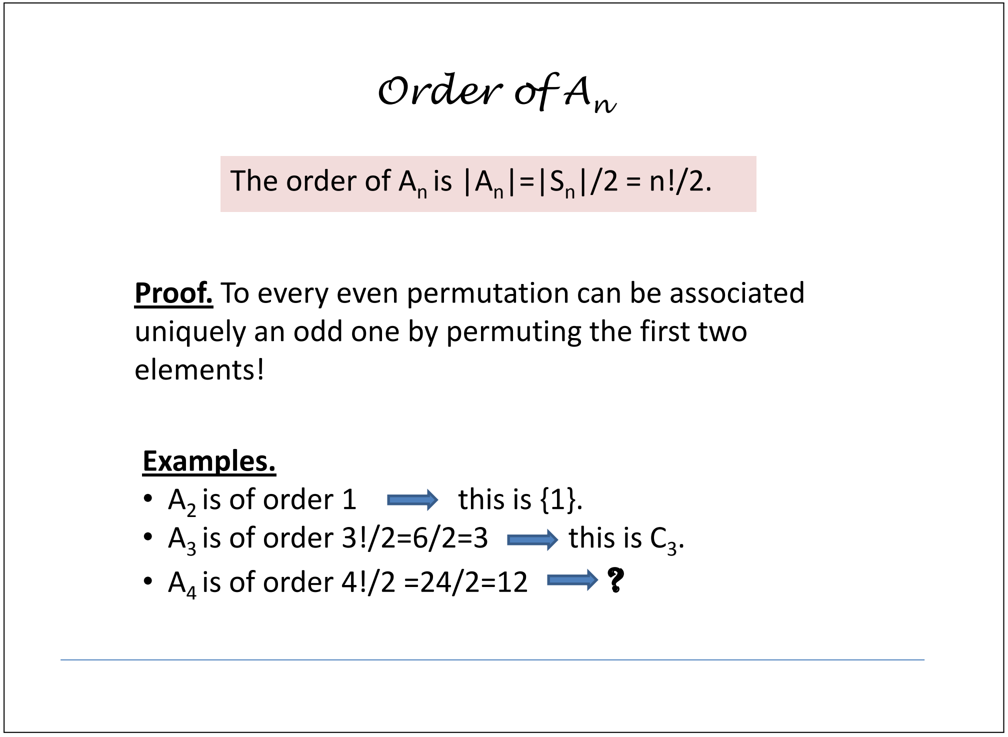


Example: A_3

	()	(12)	(23)	(13)	(123)	(132)
()	()	(1,2)	(2,3)	(1,3)	(123)	(132)
(1,2)	(1,2)	()	(123)	(132)	(2,3)	(1,3)
(2,3)	(2,3)	(132)	()	(123)	(1,3)	(1,2)
(1,3)	(1,3)	(123)	(132)	()	(1,2)	(2,3)
(123)	(123)	(1,3)	(1,2)	(2,3)	(132)	()
(132)	(132)	(2,3)	(1,3)	(1,2)	()	(123)

	()	(123)	(132)
()	()	(123)	(132)
(123)	(123)	(132)	()
(132)	(132)	()	(123)

It is the cyclic group of order 3!



Order of A_n

The order of A_n is $|A_n|=|S_n|/2 = n!/2$.

Proof. To every even permutation can be associated uniquely an odd one by permuting the first two elements!

Examples.

- A_2 is of order 1 → this is {1}.
- A_3 is of order 3!/2=6/2=3 → this is C_3.
- A_4 is of order 4!/2 =24/2=12 → ?

Question 2: one more Bad News ??

QUESTION 2: are there finite groups which are not isomorphic to planar isometries (cyclic or dihedral groups)?

Order	abelian groups	non-abelian groups
1	{1}	x
2	**$C_2 = S_2$**	x
3	C_3	x
4	C_4, Klein group	x
5	C_5	x
6	C_6	**$D_3 = S_3$**
7	C_7	x
8	C_8	D_4
12	C_{12}	D_6, A_4

Order of Elements in A_4

- Lagrange Theorem tells us: 1,2,3,4,6,12.
- In fact: 3 elements of order 2, namely (12)(34), (13)(24), (14)(23)
- And 8 elements of order 3, namely (123),(132),(124),(142),(134),(143),(234),(243)

A_4 and D_6 are not isomorphic!

http://kristin-williams.blogspot.com/2009/09/yeah.html

Exercises for Chapter 7

Exercise 36. Let σ be a permutation on 5 elements given by $\sigma = (15243)$. Compute $\text{sign}(\sigma)$ (that is, the parity of the permutation).

Exercise 37.

1. Show that any permutation of the form (ijk) is always contained in the alternating group A_n, $n \geq 3$.
2. Deduce that A_n is a non-abelian group for $n \geq 4$.

Exercise 38. Let $H = \{\sigma \in S_5 \mid \sigma(1) = 1,\ \sigma(3) = 3\}$. Is H a subgroup of S_5?

Exercise 39. In the lecture, we gave the main steps to show that the group D_6 cannot be isomorphic to the group A_4, though both of them are of order 12 and non-abelian. This exercise is about filling some of the missing details.

- Check that $(1\ 2)(3\ 4)$ is indeed of order 2.
- Check that $(1\ 2\ 3)$ is indeed of order 3.
- By looking at the possible orders of elements of D_6, prove that A_4 and D_6 cannot be isomorphic.

Chapter 8

Cayley Theorem and Puzzles

> *"As for everything else, so for a mathematical theory: beauty can be perceived but not explained."(Arthur Cayley)*

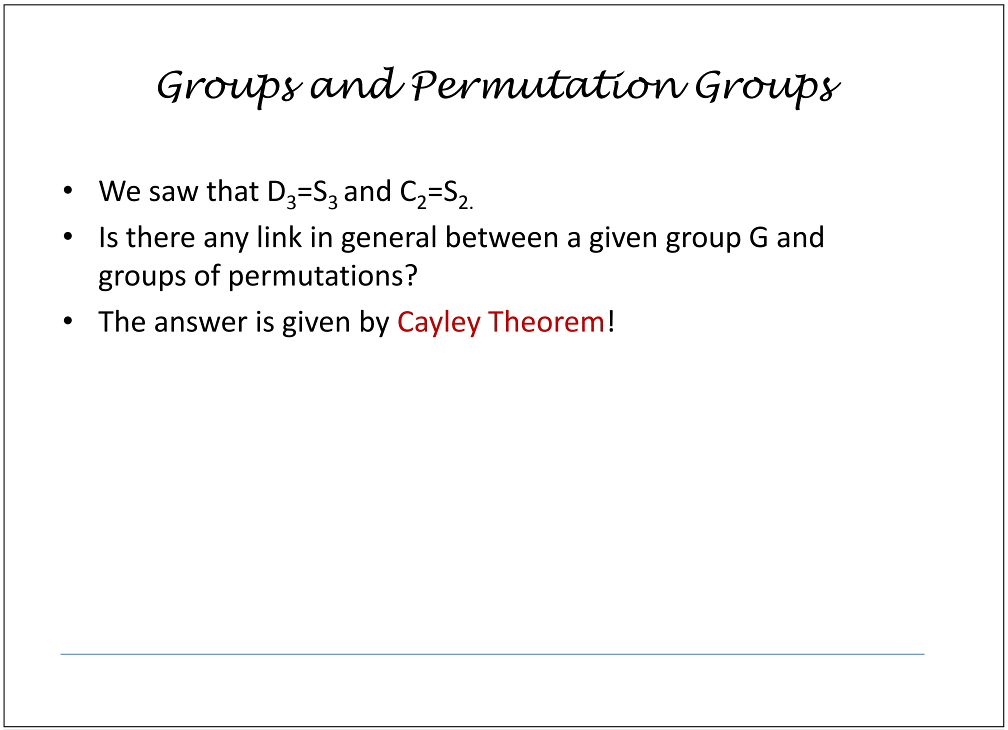
We have seen that the symmetric group S_n of all the permutations of n objects has order $n!$, and that the dihedral group D_3 of symmetries of the equilateral triangle is isomorphic to S_3, while the cyclic group C_2 is isomorphic to S_2. We now wonder whether there are more connections between finite groups and the group S_n. There is in fact a very powerful one, known as Cayley Theorem:

Theorem 15. *Every finite group is isomorphic to a group of permutations (that is to some subgroup of S_n).*

This might be surprising but recall that given any finite group $G = \{g_1, g_2, \ldots, g_n\}$, every row of its Cayley table

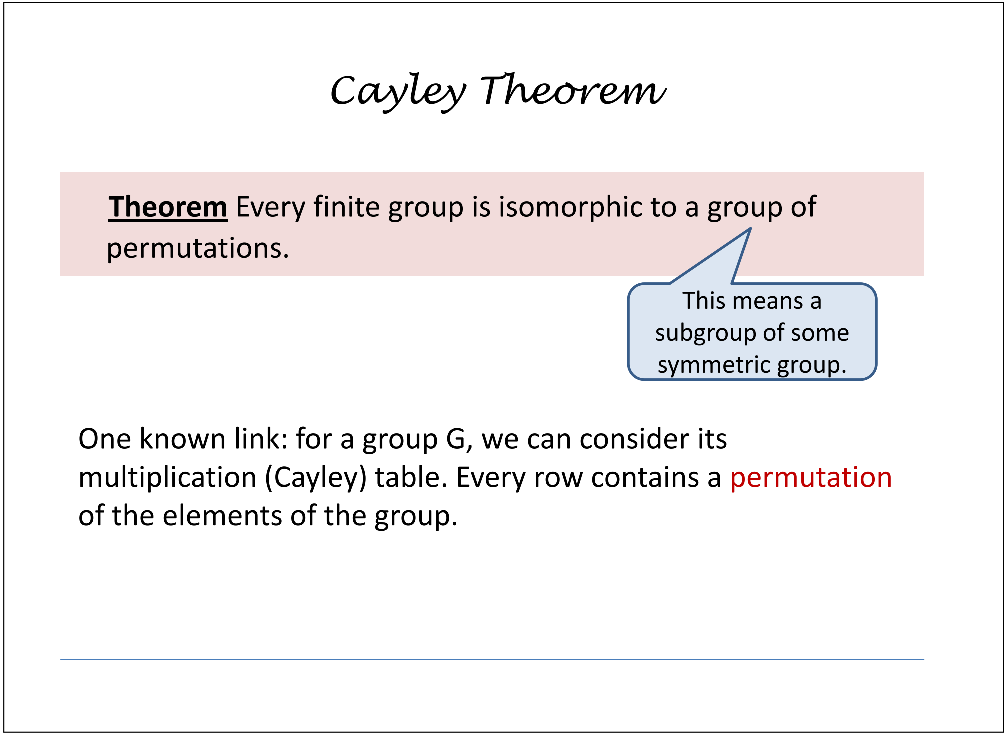
	$g_1 = e$	g_2	g_3	$\cdots$	g_n
g_1					
g_2					
$\vdots$					
g_r	g_rg_1	g_rg_2	g_rg_3	$\cdots$	g_rg_n
$\vdots$					
g_n					

is simply a permutation of the elements of G ($g_rg_s \in \{g_1, g_2, \ldots, g_n\}$).



Groups and Permutation Groups

- We saw that $D_3=S_3$ and $C_2=S_2$.
- Is there any link in general between a given group G and groups of permutations?
- The answer is given by Cayley Theorem!



Cayley Theorem

Theorem Every finite group is isomorphic to a group of permutations.

This means a subgroup of some symmetric group.

One known link: for a group G, we can consider its multiplication (Cayley) table. Every row contains a permutation of the elements of the group.

Proof. Let $(G, \cdot)$ be a group. We shall exhibit a group of permutations $(\Sigma, \circ)$ that is isomorphic to G. We have seen that the Cayley table of $(G, \cdot)$ has rows that are permutations of $\{g_1, g_2, \ldots, g_n\}$, the elements of G. Therefore let us define

$$\Sigma = \{\sigma_g : G \to G,\ \sigma_g(x) = gx,\ \forall x \in G\}$$

for $g \in G$. In words we consider the permutation maps given by the rows of the Cayley table. We verify that Σ is a group under map composition.

1. To prove that Σ is closed under composition, we will to prove that

   $$\sigma_{g_2} \circ \sigma_{g_1} = \sigma_{g_2 g_1},\ g_1 \in G,\ g_2 \in G.$$

   Indeed, for every $x \in G$,

   $$\sigma_{g_2}(\sigma_{g_1}(x)) = \sigma_{g_2}(g_1 x) = g_2(g_1 x) = (g_2 g_1)x = \sigma_{g_2 g_1}(x) \in \Sigma$$

   since $g_2 g_1 \in G$.

2. Map composition is associative.

3. The identity element is $\sigma_e(x) = ex$, since

   $$\sigma_g \circ \sigma_e = \sigma_{g \cdot e} = \sigma_g, \sigma_e \circ \sigma_g = \sigma_{e \cdot g} = \sigma_g.$$

4. The inverse. Consider g and g^{-1}, we have $gg^{-1} = g^{-1}g = e$. From

   $$\sigma_{g_2} \circ \sigma_{g_1} = \sigma_{g_2 g_1}$$

   we have

   $$\sigma_g \circ \sigma_{g^{-1}} = \sigma_e = \sigma_{g^{-1}} \circ \sigma_g.$$

Now we claim that $(G, \cdot)$ and $(\sum, \circ)$ are **isomorphic**, where the group isomorphism is given by

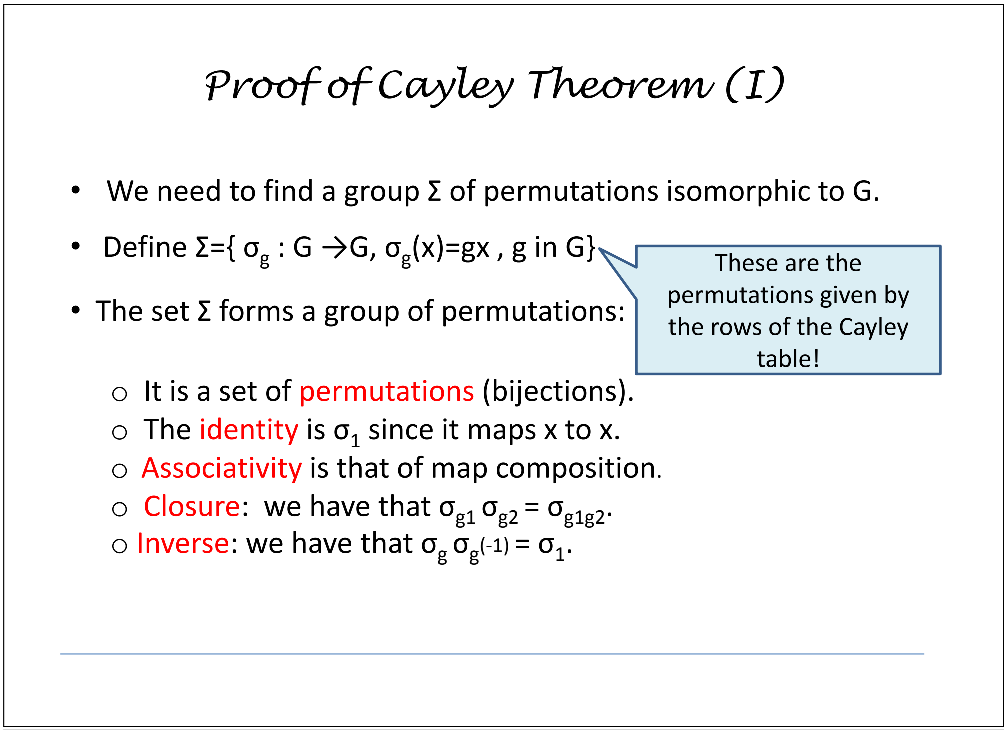
$$\phi : G \to \Sigma,\ g \mapsto \sigma_g.$$

Clearly if $\sigma_{g_1} = \sigma_{g_2}$ then $g_1 e = g_2 e \Rightarrow g_1 = g_2$. If $g_1 = g_2$, then $\sigma_{g_1} = \sigma_{g_2}$. Hence the map is one-to-one and onto, by construction!

Let us check that ϕ is a group homomorphism. If $g_1, g_2 \in G$,

$$\phi(g_1 g_2) = \sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2} = \phi(g_1) \circ \phi(g_2),$$

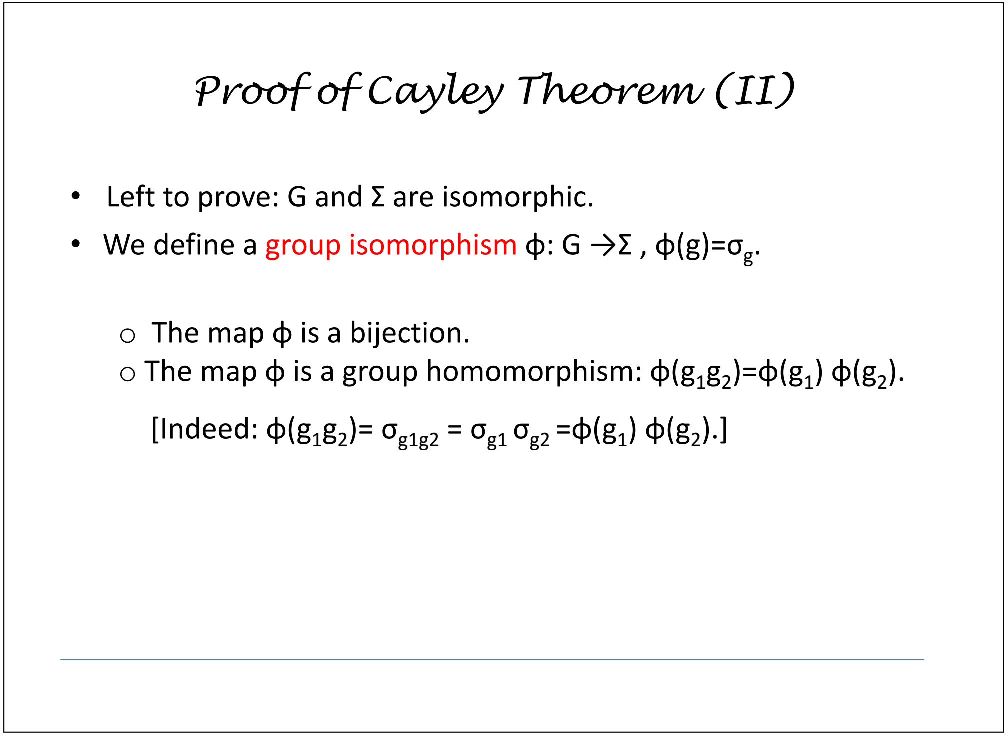
and hence we are done, ϕ is an isomorphism between $(G, \cdot)$ and a permutation group! $\square$



Proof of Cayley Theorem (I)

- We need to find a group Σ of permutations isomorphic to G.
- Define $\Sigma=\{ \sigma_g : G \rightarrow G, \sigma_g(x)=gx , g \text{ in } G\}$
- The set Σ forms a group of permutations:
  - It is a set of permutations (bijections).
  - The identity is σ_1 since it maps x to x.
  - Associativity is that of map composition.
  - Closure: we have that $\sigma_{g1}\, \sigma_{g2} = \sigma_{g1g2}$.
  - Inverse: we have that $\sigma_g\, \sigma_{g^{(-1)}} = \sigma_1$.

These are the permutations given by the rows of the Cayley table!



Proof of Cayley Theorem (II)

- Left to prove: G and Σ are isomorphic.
- We define a group isomorphism $\phi: G \rightarrow \Sigma , \phi(g)=\sigma_g$.
  - The map ϕ is a bijection.
  - The map ϕ is a group homomorphism: $\phi(g_1g_2)=\phi(g_1)\, \phi(g_2)$.

    [Indeed: $\phi(g_1g_2)= \sigma_{g1g2} = \sigma_{g1}\, \sigma_{g2} =\phi(g_1)\, \phi(g_2)$.]

Now that we saw that all finite groups are subgroups of S_n, we can understand better why we could describe the symmetries of bounded shapes by the cyclic group C_n or the dihedral group D_n which can be mapped in a natural way to permutations of the vertex locations in the plane.

Example 30. Consider the group of integers modulo 3, whose Cayley table is

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We have $\sigma_0(x) = x + 0$ corresponding to the permutation identity (). Then $\sigma_1(x) = x + 1$ corresponding to the permutation (123), $\sigma_2(x) = x + 2$ corresponding to (132).

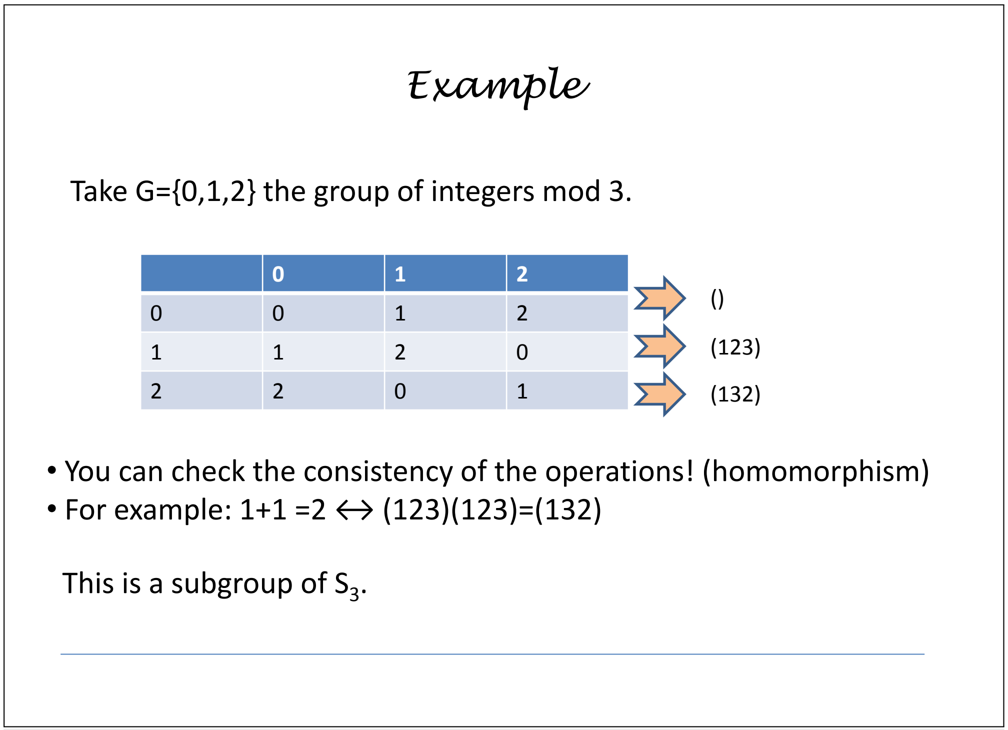
Since we have a group homomorphism, addition in $G = \{\bar{0}, \bar{1}, \bar{2}\}$ corresponds to composition in $\Sigma = \{\sigma_0, \sigma_1, \sigma_2\}$. For example

$$\bar{1} + \bar{1} = \bar{2} \iff (123)(123) = (132).$$

We next illustrate how the techniques we learnt from group theory can be used to solve puzzles. We start with the **15 puzzle**. The goal is to obtain a configuration where the 14 and 15 have been switched.

Since this puzzle involves 16 numbers, we can look at it in terms of permutations of 16 elements.

Let us assume that when the game starts, the empty space is in position 16. Every move consists of switching the empty space 16 and some other piece. To switch 14 and 15, we need to obtain the permutation (14 15) as a product of transpositions, each involving the empty space 16. Now the permutation (14 15) has parity -1, while the product of transpositions will always have parity 1, since 16 must go back to its original position, and thus no matter which moves are done, the number of vertical moves are even, and the number of horizontal moves are even as well.



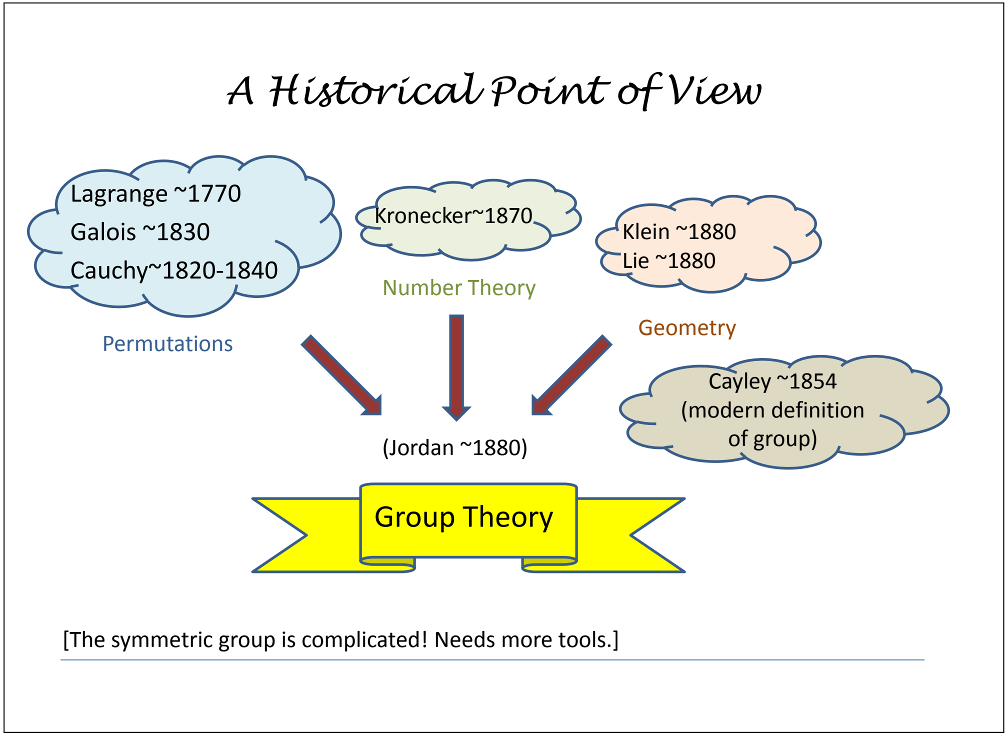
Example

Take G={0,1,2} the group of integers mod 3.

	0	1	2	
0	0	1	2	()
1	1	2	0	(123)
2	2	0	1	(132)

- You can check the consistency of the operations! (homomorphism)
- For example: 1+1 =2 ↔ (123)(123)=(132)

This is a subgroup of S_3.



A Historical Point of View

[The symmetric group is complicated! Needs more tools.]

Some Applications

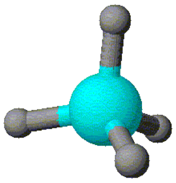
- Symmetries
- Cryptography
- Puzzles

Symmetries

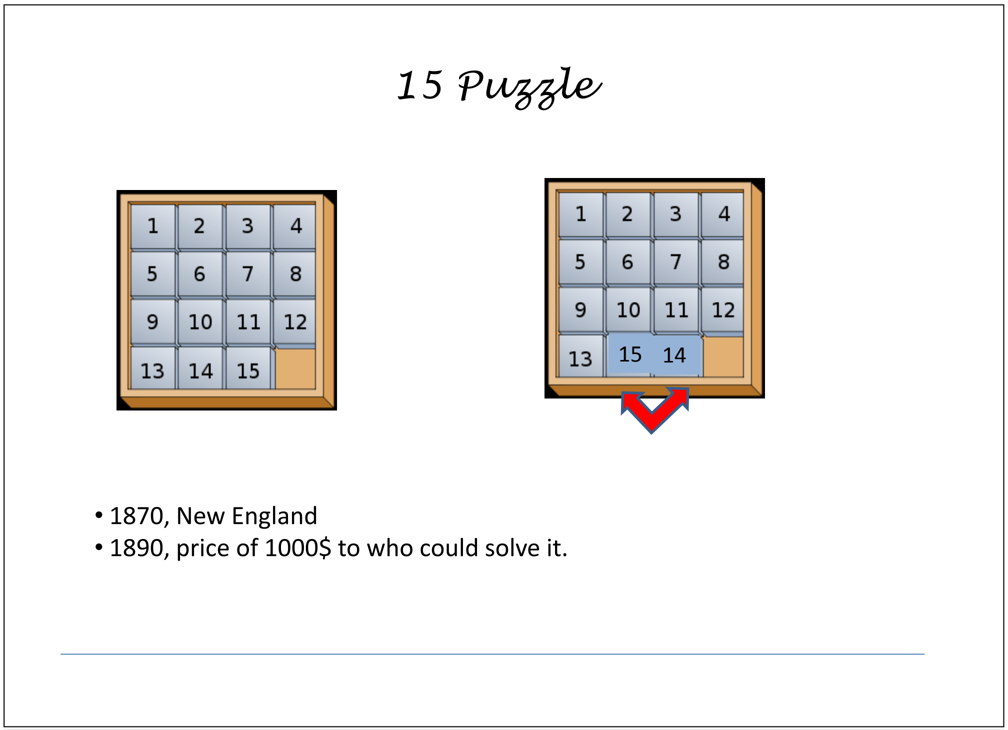
One of the main focuses of this class

- Symmetries of finite planar shapes (cyclic and dihedral groups)
- Symmetries of some infinite planar shapes (Frieze groups, later!)

One could also study symmetries of 3-dimensional shapes!

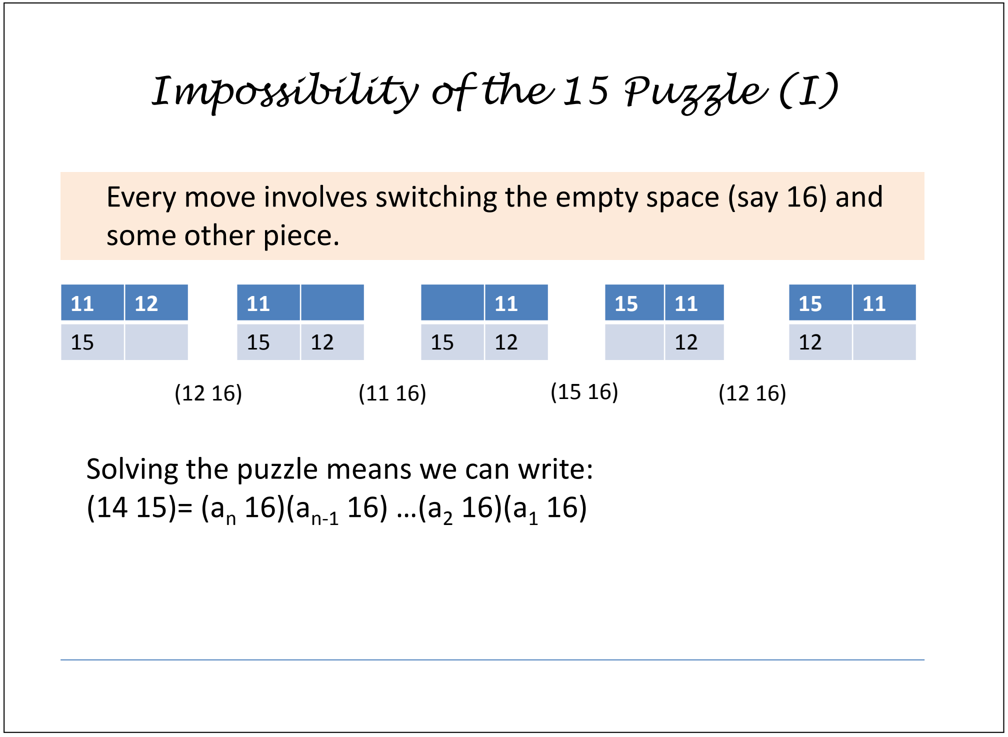


A tetrahedral AB_4 molecule (ex. methane CH_4) with symmetric group A_4.



15 Puzzle

- 1870, New England
- 1890, price of 1000$ to who could solve it.



Impossibility of the 15 Puzzle (I)

Every move involves switching the empty space (say 16) and some other piece.

11	12
15	

(12 16)

11	
15	12

(11 16)

	11
15	12

(15 16)

15	11
	12

(12 16)

15	11
12	

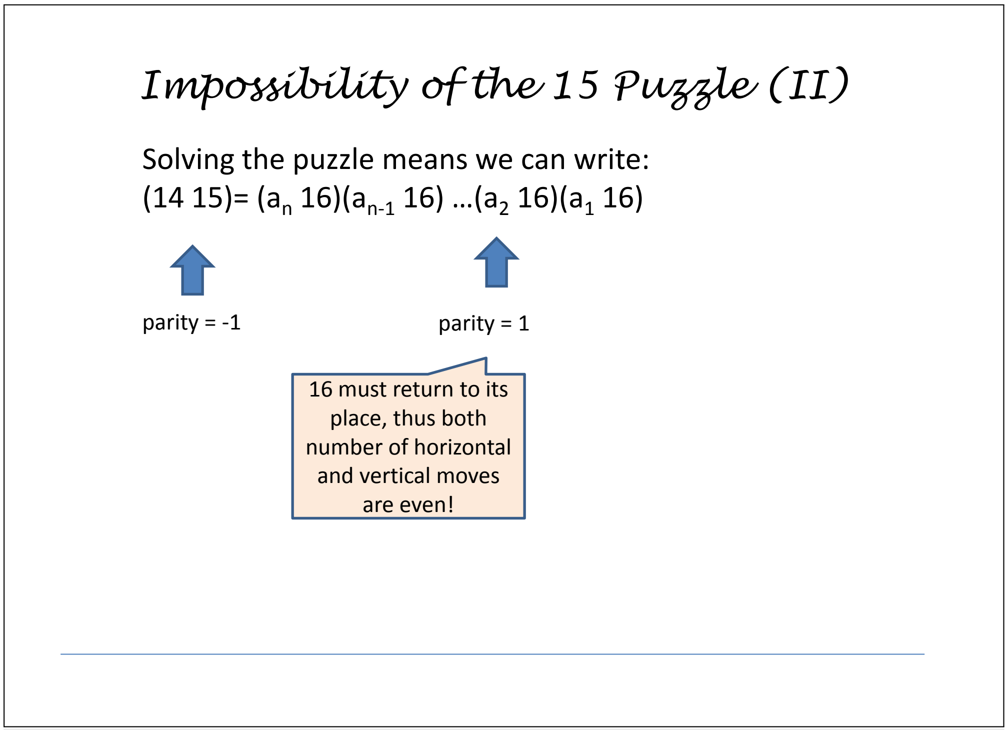
Solving the puzzle means we can write:

$(14\ 15) = (a_n\ 16)(a_{n-1}\ 16)\ \dots (a_2\ 16)(a_1\ 16)$

We next consider a **solitaire puzzle**. The goal of the game is to finish with a single stone in the middle of the board. This does not seem very easy! We might ask whether it would be easier to finish the game by having a single stone anywhere instead. To answer this question, we consider the Klein group, and label every position of the board with an element of the Klein group, such that two adjacent cells multiplied together give as result the label of the third cell (this is done both horizontally and vertically). The value of the board is given by multiplying all the group elements corresponding to board positions where a stone is. The key observation is that the value does not change when a move is made.

When the game starts, and only one stone is missing in the middle, the total value of the board is h (with the labeling shown on the slides). Since a move does not change the total value, we can only be left with a position containing an h. Since the board is unchanged under horizontal and vertical reflections, as well as under rotations by 90, 180, and 270 degrees, this further restricts the possible positions containing a valid h, and in fact, the easiest version is as hard as the original game!

Other applications of group theory can be found in the area of cryptography. We already saw Caesar cipher, and affine ciphers. We will see some more: (1) check digits and (2) the RSA cryptosystem.



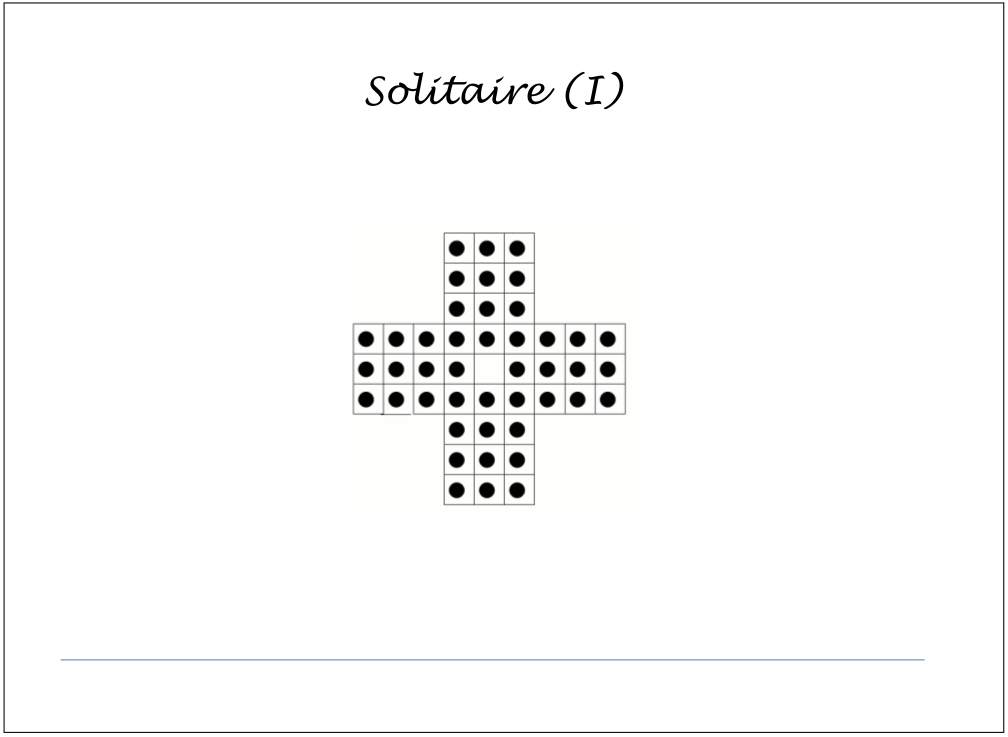
Impossibility of the 15 Puzzle (II)

Solving the puzzle means we can write:
$(14\ 15) = (a_n\ 16)(a_{n-1}\ 16) \ldots (a_2\ 16)(a_1\ 16)$

parity = -1

parity = 1

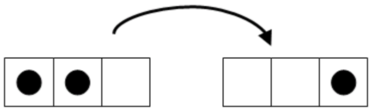
16 must return to its place, thus both number of horizontal and vertical moves are even!



Solitaire (I)

Solitaire (II)

- **A *move*** = pick up a marble, jump it horizontally or vertically (but *not* diagonally) over a single marble into a vacant hole, removing the marble that was jumped over.



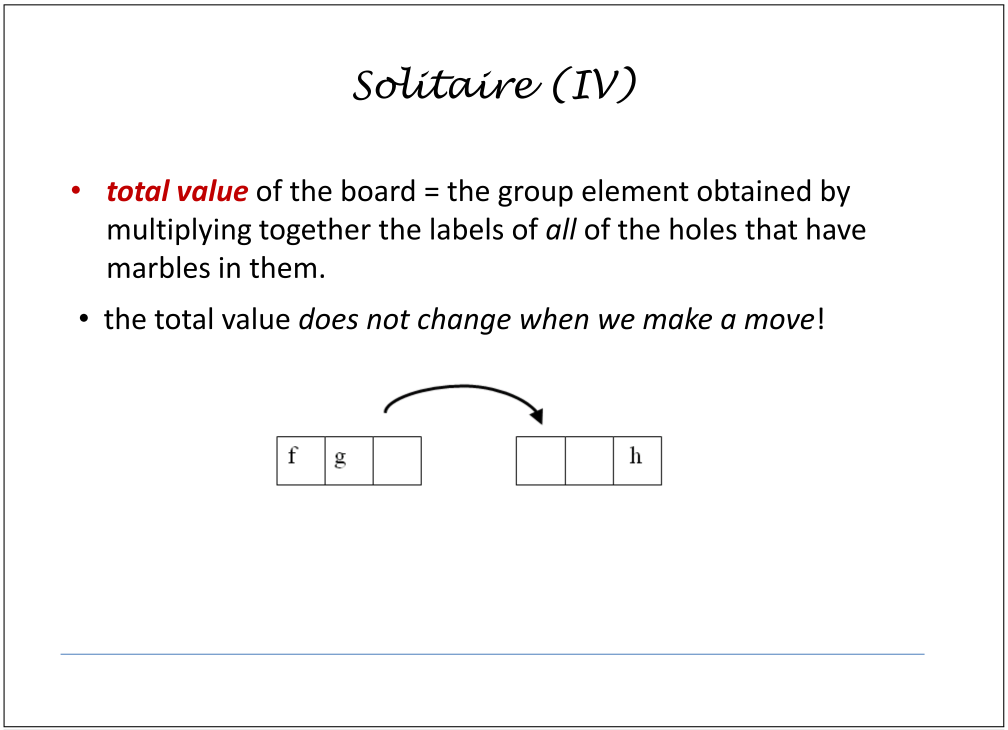
- **A win** = finish with a single marble left in the central hole.
- Would it be **easier** if a win = finish with a single marble *anywhere*?

Solitaire (III)

			f	g	h			
			g	h	f			
			h	f	g			
f	g	h	f	g	h	f	g	h
g	h	f	g	h	f	g	h	f
h	f	g	h	f	g	h	f	g
			f	g	h			
			g	h	f			
			h	f	g			

- G={1,f,g,h} = **Klein group**
- Label the board such that labels of two cells multiplied together give the label of the third cell.

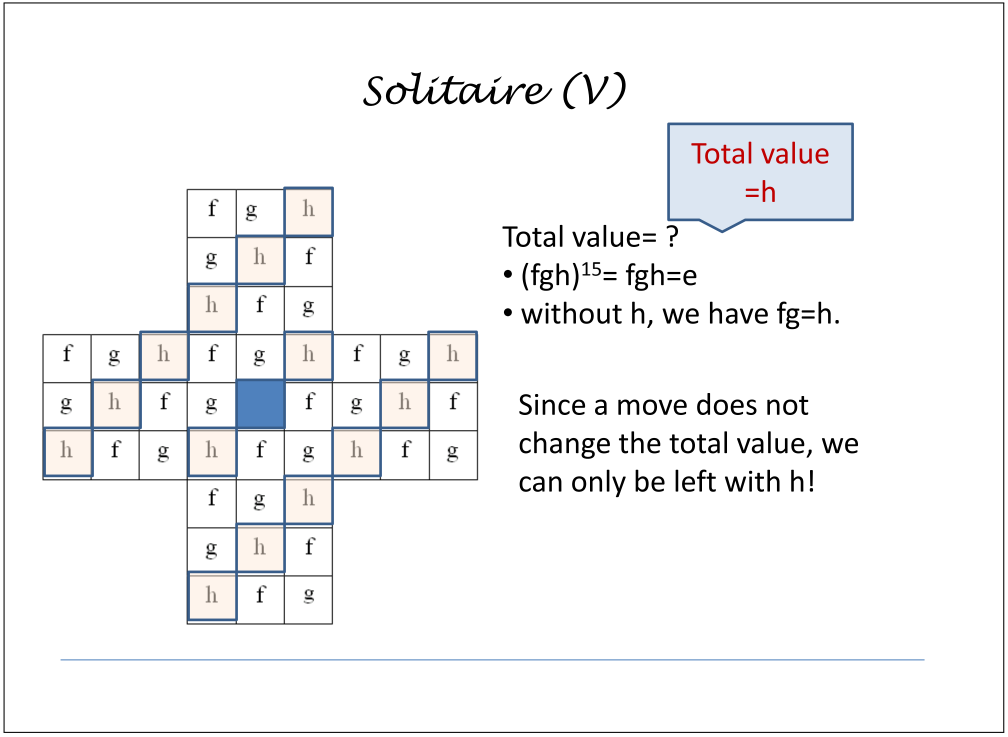
Binary operation of the Klein group



Solitaire (IV)

- ***total value*** of the board = the group element obtained by multiplying together the labels of *all* of the holes that have marbles in them.
- the total value *does not change when we make a move*!

f	g				h



Solitaire (V)

			f	g	h			
			g	h	f			
			h	f	g			
f	g	h	f	g	h	f	g	h
g	h	f	g		f	g	h	f
h	f	g	h	f	g	h	f	g
			f	g	h			
			g	h	f			
			h	f	g			

Total value =h

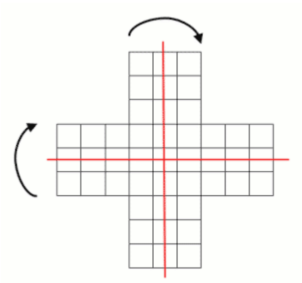
Total value= ?

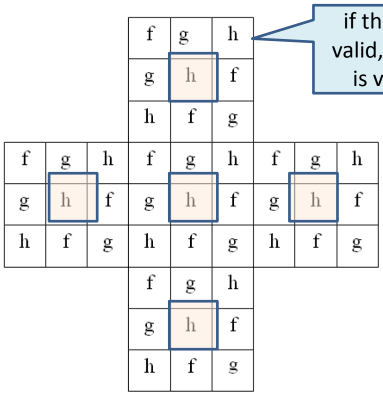
- $(fgh)^{15}$= fgh=e
- without h, we have fg=h.

Since a move does not change the total value, we can only be left with h!

Solitaire (VI)

A Solitaire board is unchanged under reflection in the horizontal and vertical axes, and rotation through 90°, 180°, 270° and 360°.

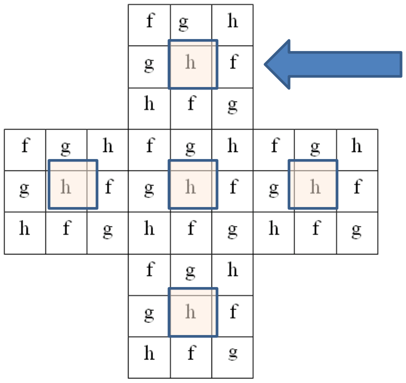




			f	g	h			
			g	h	f			
			h	f	g			
f	g	h	f	g	h	f	g	h
g	h	f	g	h	f	g	h	f
h	f	g	h	f	g	h	f	g
			f	g	h			
			g	h	f			
			h	f	g			

if this h is valid, then f is valid!

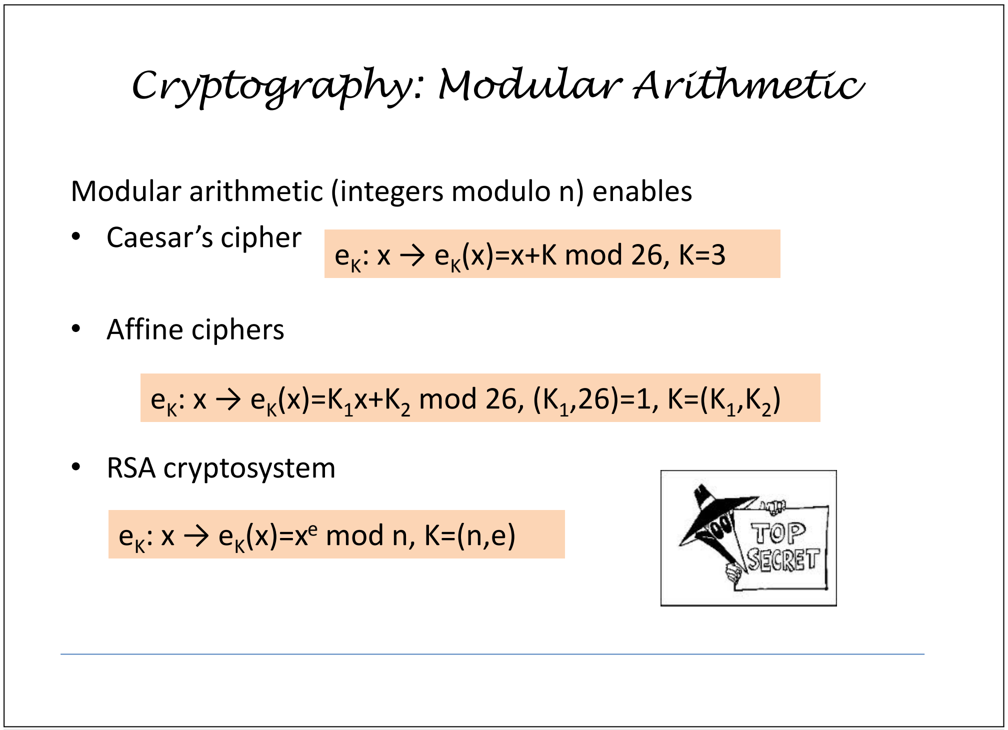
Solitaire (VII)



			f	g	h			
			g	h	f			
			h	f	g			
f	g	h	f	g	h	f	g	h
g	h	f	g	h	f	g	h	f
h	f	g	h	f	g	h	f	g
			f	g	h			
			g	h	f			
			h	f	g			

If we can solve this position, then we can solve the middle one!

We just shown: the "easiest version" is as hard!!



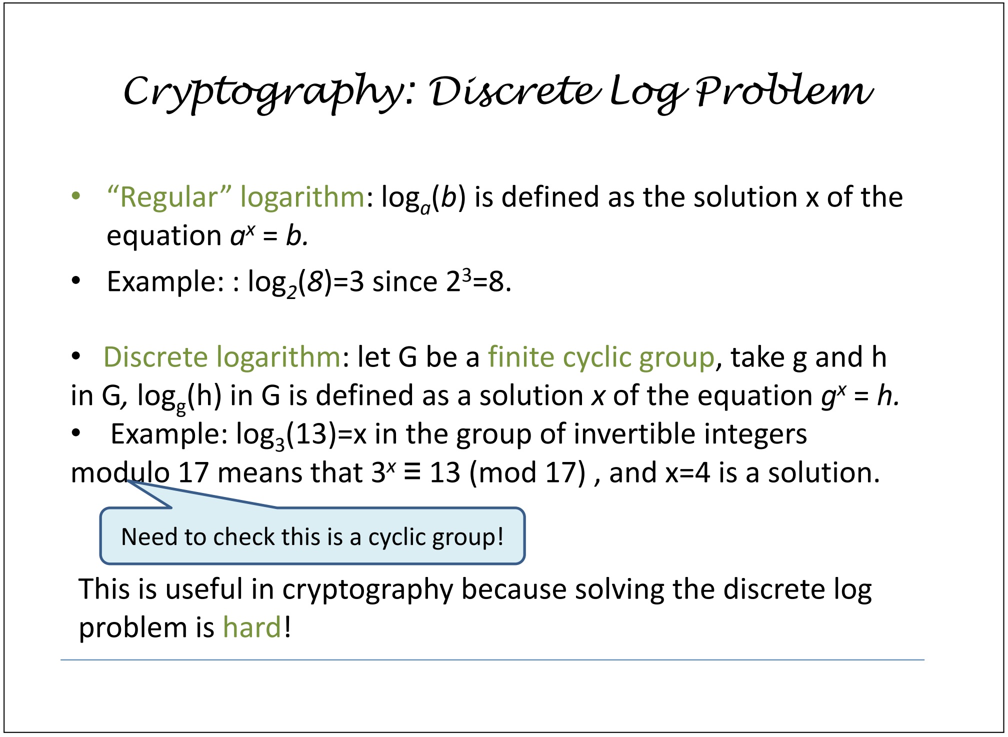
Cryptography: Modular Arithmetic

Modular arithmetic (integers modulo n) enables

- Caesar's cipher $e_K: x \to e_K(x)=x+K \bmod 26, K=3$
- Affine ciphers

  $e_K: x \to e_K(x)=K_1x+K_2 \bmod 26, (K_1,26)=1, K=(K_1,K_2)$
- RSA cryptosystem

  $e_K: x \to e_K(x)=x^e \bmod n, K=(n,e)$



Cryptography: Discrete Log Problem

- "Regular" logarithm: $\log_a(b)$ is defined as the solution x of the equation $a^x = b$.
- Example: : $\log_2(8)=3$ since $2^3=8$.

- Discrete logarithm: let G be a finite cyclic group, take g and h in G, $\log_g(h)$ in G is defined as a solution x of the equation $g^x = h$.
- Example: $\log_3(13)=x$ in the group of invertible integers modulo 17 means that $3^x \equiv 13 \pmod{17}$, and x=4 is a solution.

Need to check this is a cyclic group!

This is useful in cryptography because solving the discrete log problem is hard!

Cryptography: Check Digit (I)

Take a message formed by a string of digits.

A **check digit** consists of a single digit, computed from the other digits, appended at the end of the message.

It is a form of redundancy to enable error detection.

We will look at the Check Digit introduced by J. Verhoeff in 1969, based on the dihedral group D_5.

Cryptography: Check Digit (II)

Multiplication table of D_5 with 0=do-nothing, 1-4=rotations, 5-9=reflections, *=binary operation in D_5.

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Cryptography: Check Digit (III)

How does it work?Let σ be a permutation in S_{10}. To any string $a_1a_2\ldots a_{n-1}$ of digits, we append the check digit a_n so that $\sigma(a_1) * \sigma^2(a_2) * \ldots * \sigma^{n-1}(a_{n-1}) * \sigma^n(a_n) = 0$.

Composition of the permutation σ

Binary operation of D_5

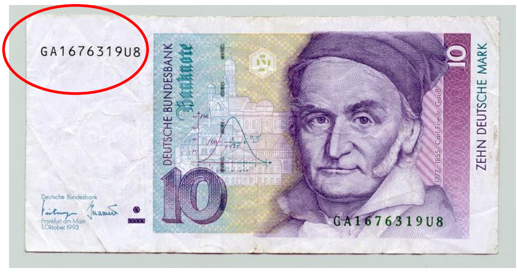
Single-digit errors are detected: if the digit a is replaced by b, then $\sigma^i(a)$ is replaced by $\sigma^i(b)$ ($\sigma^i(a) \neq \sigma^i(b)$ when a≠b) thus the check digit is changed and an error is detected.

Cryptography: Check Digit (IV)

Example. Take σ=(1,7,9)(2,5,10,4,6) and the digit 12345 (n-1=5).
[23456]

- $\sigma(2)=5$, $\sigma^2(3)=3$, $\sigma^3(4)=5$, $\sigma^4(5)=2$, $\sigma^5(6)=6$.
- $5*3*5*2*6*\sigma^6(a_6)=0 \Rightarrow 5*\sigma^6(a_6)=0 \Rightarrow \sigma^6(a_6)= 5$ and $a_6=2$.
- We get [234562] that is 123451.

Check digit 8 on a German banknote.

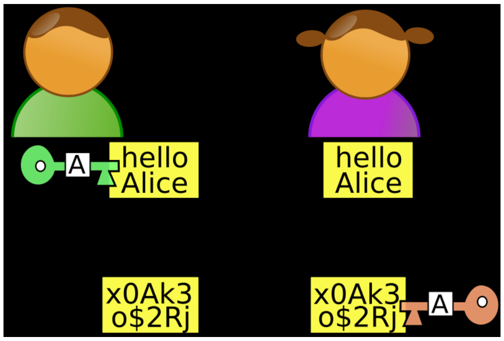


Application of Euler Theorem: RSA

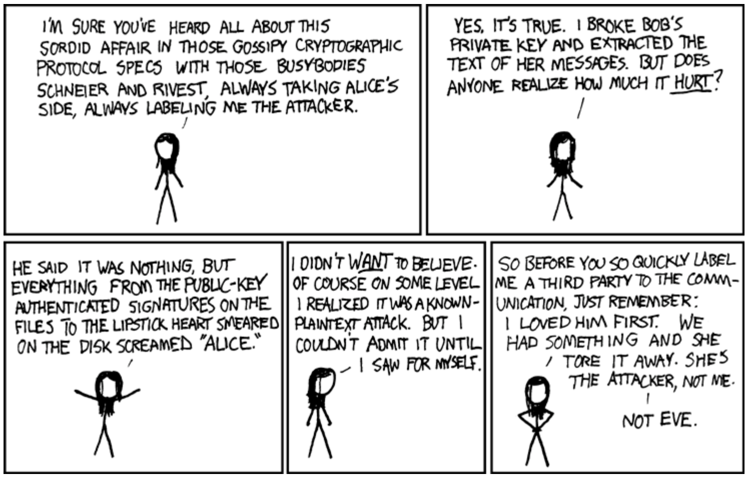
RSA is an encryption scheme discovered by River, Shamir and Adleman (in 1978).

Alice and Bob Story

Alice and Bob want to exchange confidential data in the presence of an eavesdropper Eve.



Alice and Bob story by xkcd


I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.
YES, IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?
HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SMEARED ON THE DISK SCREAMED "ALICE."
I DIDN'T WANT TO BELIEVE. OF COURSE ON SOME LEVEL I REALIZED IT WAS A KNOWN-PLAINTEXT ATTACK. BUT I COULDN'T ADMIT IT UNTIL I SAW FOR MYSELF.
SO BEFORE YOU SO QUICKLY LABEL ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER: I LOVED HIM FIRST. WE HAD SOMETHING AND SHE TORE IT AWAY. SHE'S THE ATTACKER, NOT ME.
NOT EVE.

RSA Protocol (I)

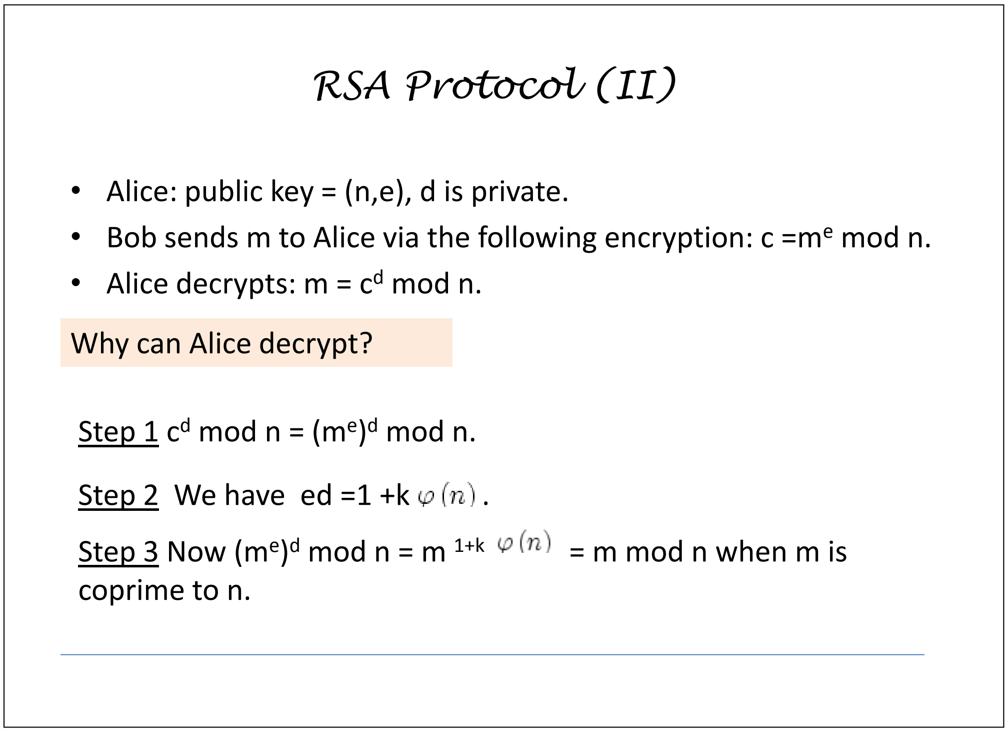
- Select two distinct large primes p and q ("large" means 100 digits ☺).
- Compute n=pq.
- The Euler totient function of n is $\varphi(n)$ = (p-1)(q-1).

This function counts the integers coprime to n.

- Pick an odd integer e such that e is coprime to $\varphi(n)$.
- Find d such that ed = 1 modulo $\varphi(n)$.

e exists because it is coprime to the Euler totient function!

Publish e and n as public keys, keep d private.



RSA Protocol (II)

- Alice: public key = (n,e), d is private.
- Bob sends m to Alice via the following encryption: $c = m^e \bmod n$.
- Alice decrypts: $m = c^d \bmod n$.

Why can Alice decrypt?

Step 1 $c^d \bmod n = (m^e)^d \bmod n$.

Step 2 We have $ed = 1 + k\varphi(n)$.

Step 3 Now $(m^e)^d \bmod n = m^{1+k\varphi(n)} = m \bmod n$ when m is coprime to n.

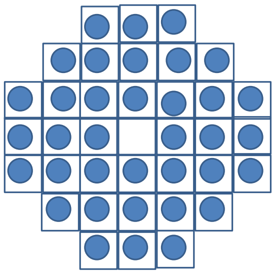
Exercises for Chapter 8

Exercise 40.

- Let G be the Klein group. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Identify this subgroup.
- Let G be the cyclic group C_4. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Identify this subgroup.

Exercise 41. Show that any rearrangement of pieces in the 15-puzzle starting from the standard configuration (pieces are ordered from 1 to 15, with the 16th position empty) which brings the empty space back to its original position must be an even permutation of the other 15 pieces.

Exercise 42. Has this following puzzle a solution? The rule of the game is the same as the solitaire seen in class, and a win is a single marble in the middle of the board. If a win is a single marble anywhere in the board, is that any easier?



Chapter 9

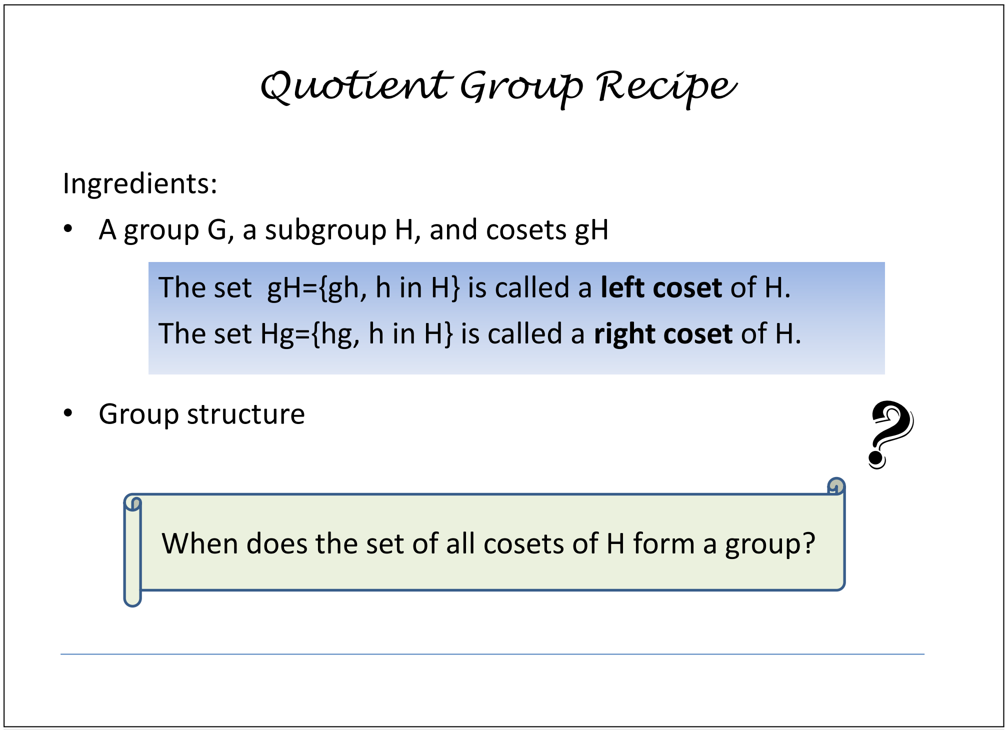
Quotient Groups

> *"Algebra is the offer made by the devil to the mathematician...All you need to do, is give me your soul: give up geometry." (Michael Atiyah)*

Based on the previous lectures, we now have the following big picture. We know that planar isometries are examples of groups, and more precisely, that finite groups of planar isometries are either cyclic groups or dihedral groups (this is Leonardo Theorem). We also know that there other groups out there, for example the alternating group, but still, most of the groups we have seen can be visualised in terms of geometry. The goal of this lecture is to introduce a standard object in abstract algebra, that of quotient group. This is likely to be the most "abstract" this class will get! Thankfully, we have already studied integers modulo n and cosets, and we can use these to help us understand the more abstract concept of quotient group.

Let us recall what a coset is. Take a group G and a subgroup H. The set $gH = \{gh,\ g \in H\}$ is a left coset of H, while $Hg = \{hg,\ h \in H\}$ is a right coset of H. Consider all the distinct cosets of G (either right or left cosets). The question is: does the set of all distinct cosets of G form a group?

Example 31. Consider $G = \{0, 1, 2, 3\}$ to be the set of integers modulo 4, and take the subgroup $H = \{0, 2\}$ (you might want to double check that you remember why this is a subgroup). We have two cosets H and $1+H = \{1, 3\}$. To have a group structure, we need to choose a binary operation. Let us say we start with $+$, the addition modulo 4. How do we add two cosets? Let us try elementwise. To compute $\{0, 2\}+\{1, 3\}$, we have $\{0+1, 0+3, 2+1, 2+3\} = \{1, 3\}$. It seems not bad, the sum of these two cosets does give another coset!



Quotient Group Recipe

Ingredients:

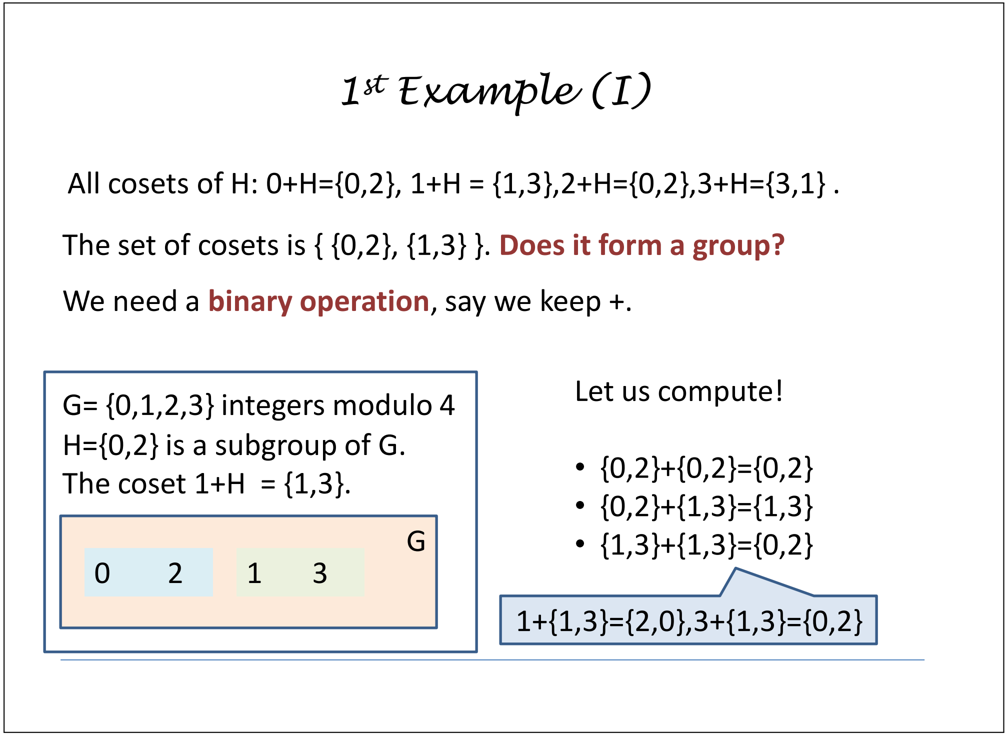
- A group G, a subgroup H, and cosets gH

The set $gH=\{gh, h \text{ in } H\}$ is called a **left coset** of H.
The set $Hg=\{hg, h \text{ in } H\}$ is called a **right coset** of H.

- Group structure

?

When does the set of all cosets of H form a group?



1^{st} Example (I)

All cosets of H: $0+H=\{0,2\}$, $1+H = \{1,3\}$, $2+H=\{0,2\}$, $3+H=\{3,1\}$.

The set of cosets is $\{ \{0,2\}, \{1,3\} \}$. **Does it form a group?**

We need a **binary operation**, say we keep $+$.

$G= \{0,1,2,3\}$ integers modulo 4
$H=\{0,2\}$ is a subgroup of G.
The coset $1+H = \{1,3\}$.

Let us compute!

- $\{0,2\}+\{0,2\}=\{0,2\}$
- $\{0,2\}+\{1,3\}=\{1,3\}$
- $\{1,3\}+\{1,3\}=\{0,2\}$

$1+\{1,3\}=\{2,0\}$, $3+\{1,3\}=\{0,2\}$

Let us try to do that with both cosets, and summarize it in a Cayley table.

	$\{0,2\}$	$\{1,3\}$
$\{0,2\}$	$\{0,2\}$	$\{1,3\}$
$\{1,3\}$	$\{1,3\}$	$\{0,2\}$

We notice that we indeed have a group structure, since the set of cosets is closed under the binary operation $+$, it has an identity element $\{0,2\}$, every element has an inverse, and associativity holds. In fact, we can see from the Cayley table that this group is in fact isomorphic to the cyclic group C_2.

In the above example, we defined a binary operation on the cosets of H, where H is a subgroup of a group $(G,+)$ by

$$(g+H)+(k+H)=\{g+h+k+h' \text{ for all } h,h'\}.$$

We now illustrate using the same example that computations could have been done with a choice of a representative instead.

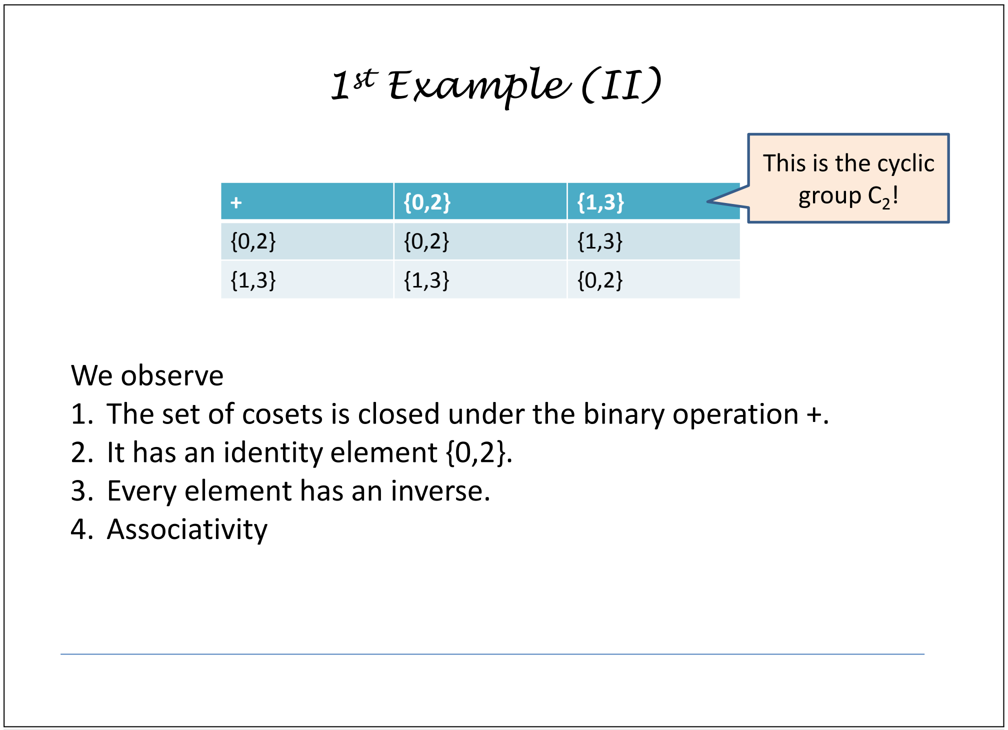
Example 32. We continue with the same setting as in Example 31. Since $0+H=\{0,2\}$ and $1+H=\{1,3\}$, we have

$$(0+H)+(1+H)=(0+1)+H=1+H$$

using the representative 0 from $0+H$ and 1 from $1+H$. Alternatively, if 2 and 3 are chosen as representatives instead, we have

$$(2+H)+(3+H)=(2+3)+H=1+H$$

since $5 \equiv 1 \mod 4$. There are in total 4 ways of choosing the coset representatives, since 0 and 2 can be chosen for the first coset, and 1 and 3 could be chosen in the second coset. Any choice will give the same answer as the sum of the two cosets.



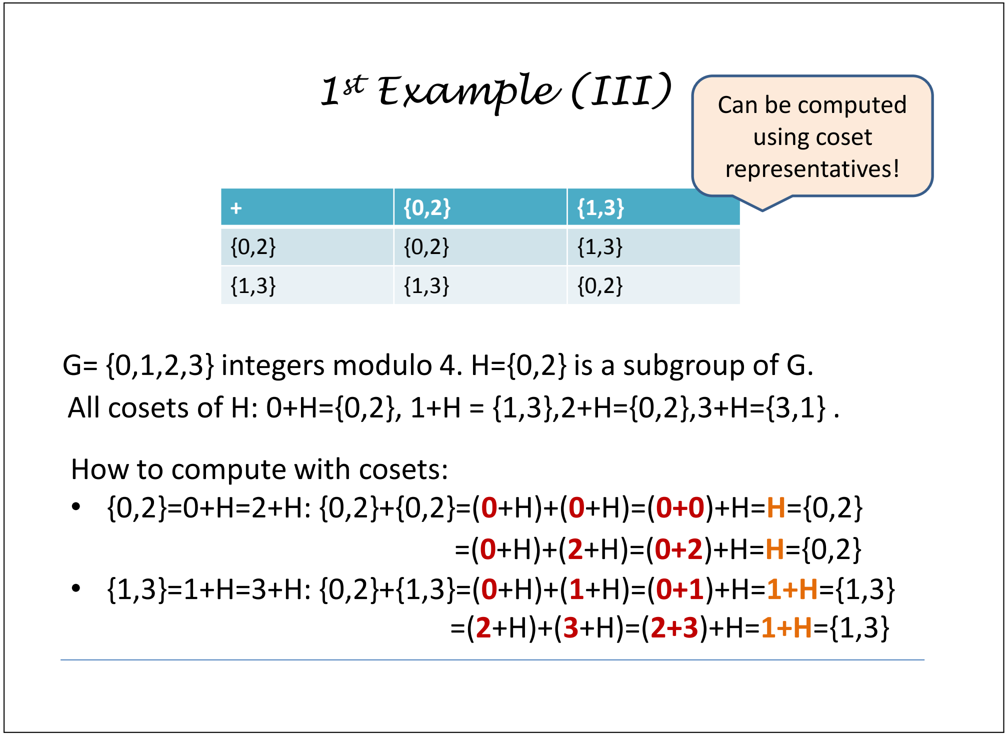
1st Example (II)

This is the cyclic group C_2!

+	{0,2}	{1,3}
{0,2}	{0,2}	{1,3}
{1,3}	{1,3}	{0,2}

We observe

1. The set of cosets is closed under the binary operation +.
2. It has an identity element {0,2}.
3. Every element has an inverse.
4. Associativity



1st Example (III)

Can be computed using coset representatives!

+	{0,2}	{1,3}
{0,2}	{0,2}	{1,3}
{1,3}	{1,3}	{0,2}

G= {0,1,2,3} integers modulo 4. H={0,2} is a subgroup of G.
All cosets of H: 0+H={0,2}, 1+H = {1,3},2+H={0,2},3+H={3,1} .

How to compute with cosets:

- {0,2}=0+H=2+H: {0,2}+{0,2}=(**0**+H)+(**0**+H)=(**0+0**)+H=**H**={0,2}
  =(**0**+H)+(**2**+H)=(**0+2**)+H=**H**={0,2}
- {1,3}=1+H=3+H: {0,2}+{1,3}=(**0**+H)+(**1**+H)=(**0+1**)+H=**1+H**={1,3}
  =(**2**+H)+(**3**+H)=(**2+3**)+H=**1+H**={1,3}

Let us now revisit integers modulo n. We recall that a and b are said to be congruent modulo n if their difference $a - b$ is an integer which is a multiple of n. We saw that being congruent mod n is an equivalence relation, and that addition modulo n is well defined, which led to the definition of group of integers modulo n with respect to addition.

Now consider the group $G = \mathbb{Z}$ of integers, and the subgroup $H = n\mathbb{Z}$, that is

$$H = n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

is the set of multiples of n (you might check that this is indeed a subgroup). We now consider the cosets of H, that is

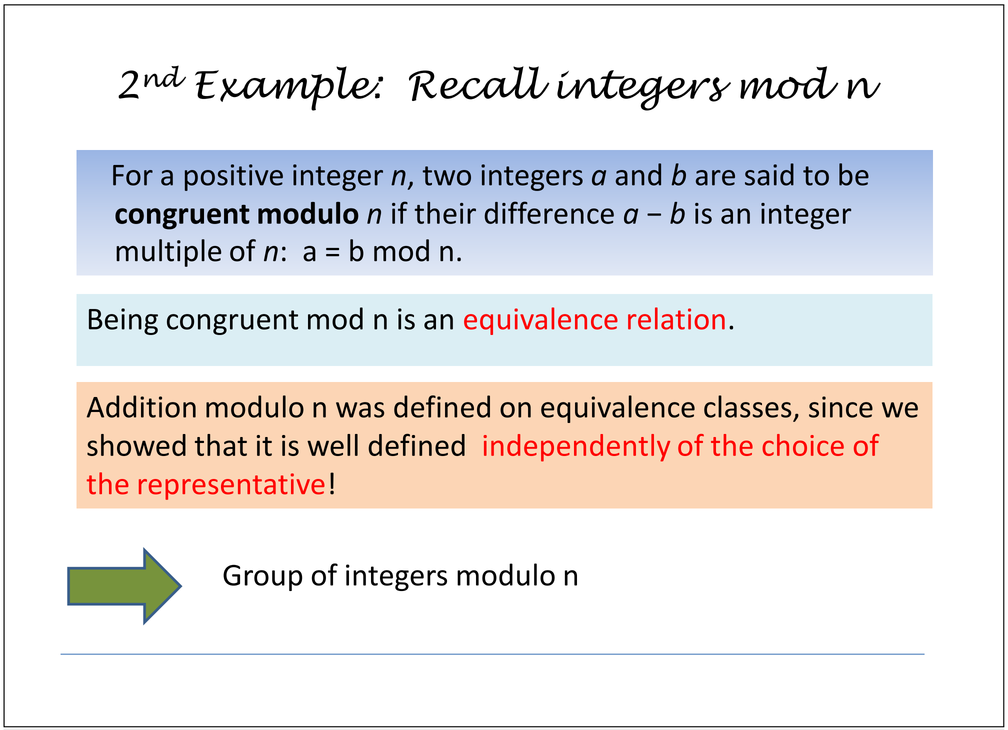
$$-2 + H, -1 + H, 0 + H, 1 + H, 2 + H, \ldots.$$

Example 33. If $n = 3$, then $H = 3\mathbb{Z}$ consists of the multiple of 3. We have exactly 3 distinct cosets, given by

$$0 + H, 1 + H, 2 + H$$

since $\mathbb{Z}$ is partitioned by these 3 cosets. Indeed, $0 + H$ contains all the multiples of 3, $1 + H$ contains all the multiples of 3 to which 1 is added, and $0 + H$ all the multiples of 3, to which 2 is added, which cover all the integers.

Now when we do computations with integers modulo 3, we choose a coset representative. When we compute $(0 \mod 3) + (1 \mod 3)$, we are looking at the sum of the coset $(0 + H)$ and of the coset $(1 + H)$.



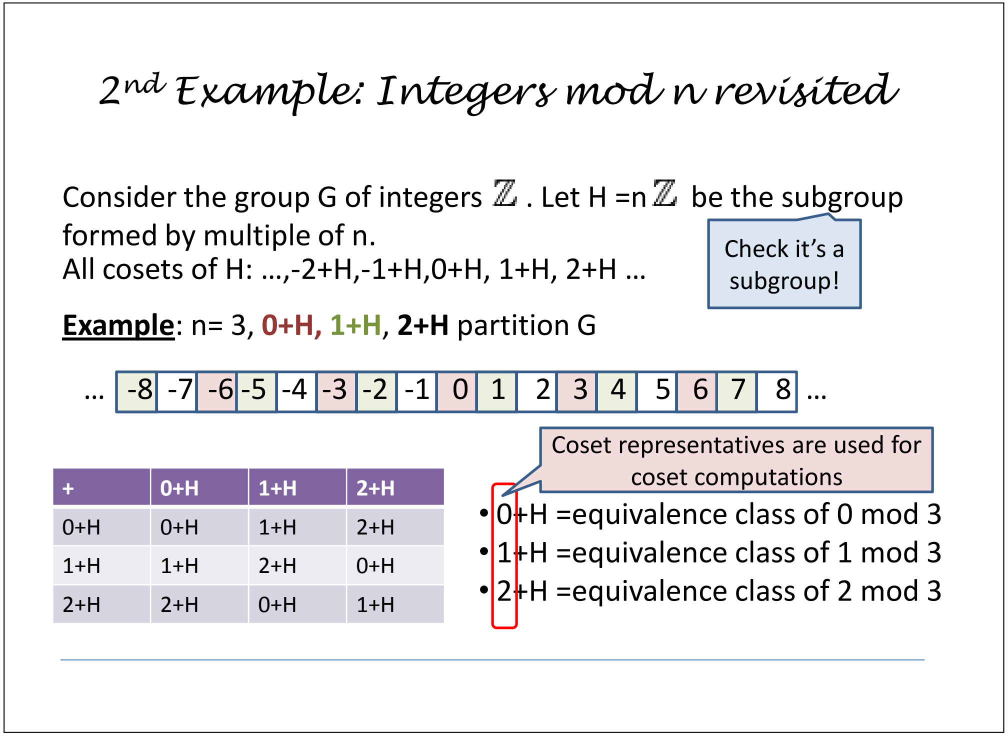
2nd Example: Recall integers mod n

For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n* if their difference *a* − *b* is an integer multiple of *n*: a = b mod n.

Being congruent mod n is an equivalence relation.

Addition modulo n was defined on equivalence classes, since we showed that it is well defined independently of the choice of the representative!

Group of integers modulo n



2nd Example: Integers mod n revisited

Consider the group G of integers $\mathbb{Z}$. Let H =n$\mathbb{Z}$ be the subgroup formed by multiple of n.
All cosets of H: …,-2+H,-1+H,0+H, 1+H, 2+H …

Check it's a subgroup!

Example: n= 3, **0+H, 1+H, 2+H** partition G

…	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	…

+	0+H	1+H	2+H
0+H	0+H	1+H	2+H
1+H	1+H	2+H	0+H
2+H	2+H	0+H	1+H

Coset representatives are used for coset computations

- 0+H =equivalence class of 0 mod 3
- 1+H =equivalence class of 1 mod 3
- 2+H =equivalence class of 2 mod 3

In the case of integers modulo n, we do have that cosets form a group. Now we may wonder whether this is true in general. To answer this question, let us take a general group G, and its set of cosets. We need to define a binary operation:

$$(gH, g'H) \mapsto (gH)(g'H)$$

multiplicatively, or

$$(g+H, g'+H) \mapsto (g+H)+(g'+H)$$

additively. Now, is the set $\{gH, g \in G\}$ closed under this binary operation, that is, is it true that

$$(gH)(g'H) = gg'H$$

multiplicatively, or

$$(g+H)+(g'+H) = (g+g')+H$$

additively. Let us see what happens multiplicatively. If we choose two elements $gh \in gH$ and $g'h' \in g'H$, then

$$(gh)(g'h') \neq gg'hh'$$

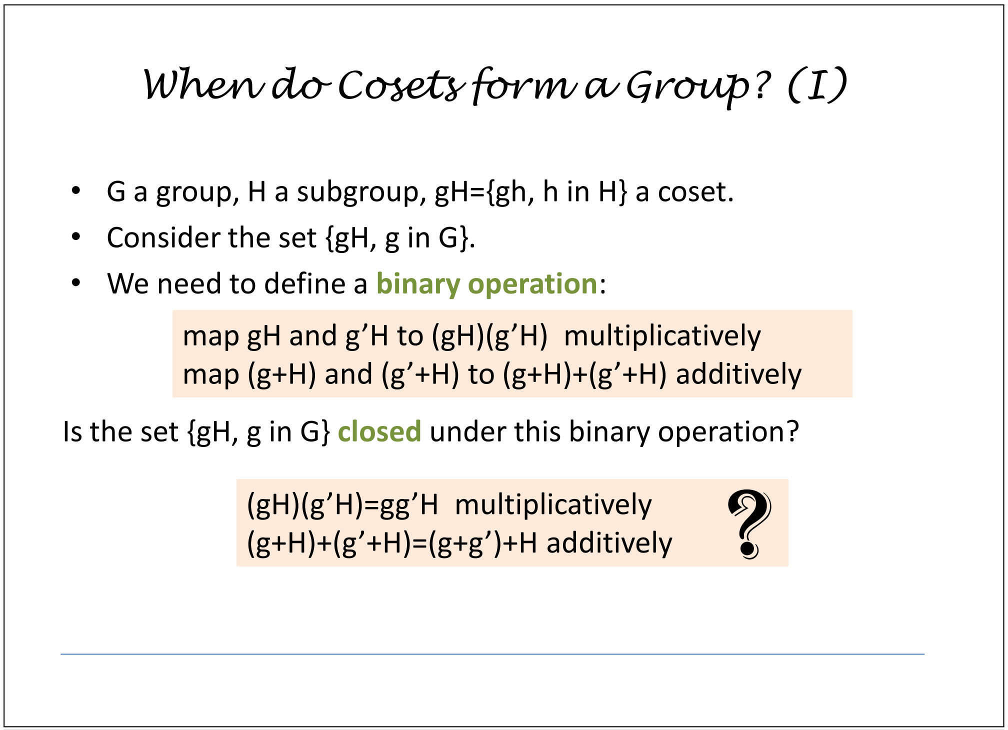
in general. We do have equality if the group is Abelian, but otherwise there is no reason for that to be true. This leads us to the following definition.

Definition 18. A subgroup H of $(G, \cdot)$ is called a normal subgroup if for all $g \in G$ we have

$$gH = Hg.$$

We shall denote that H is a subgroup of G by $H < G$, and that H is a normal subgroup of G by $H \lhd G$.

One has to be very careful here. The equality $gH = Hg$ is a set equality! It says that a right coset is equal to a left coset, it is not an equality elementwise.



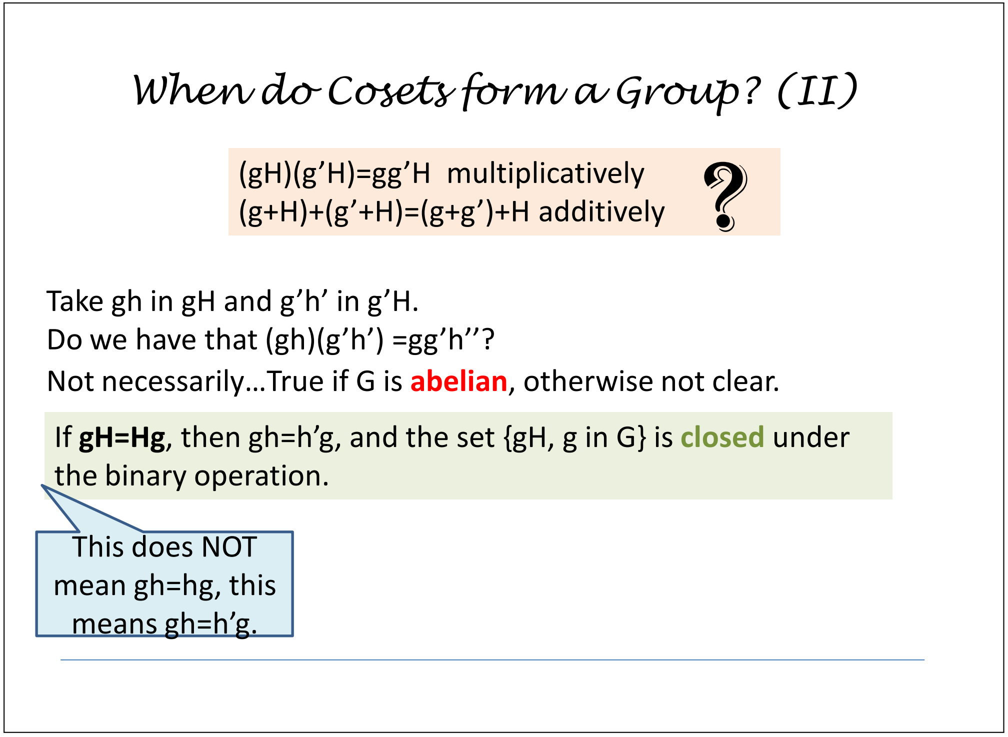
When do Cosets form a Group? (I)

- G a group, H a subgroup, gH={gh, h in H} a coset.
- Consider the set {gH, g in G}.
- We need to define a **binary operation**:

map gH and g'H to (gH)(g'H) multiplicatively
map (g+H) and (g'+H) to (g+H)+(g'+H) additively

Is the set {gH, g in G} **closed** under this binary operation?

(gH)(g'H)=gg'H multiplicatively
(g+H)+(g'+H)=(g+g')+H additively ?



When do Cosets form a Group? (II)

(gH)(g'H)=gg'H multiplicatively
(g+H)+(g'+H)=(g+g')+H additively ?

Take gh in gH and g'h' in g'H.
Do we have that (gh)(g'h') =gg'h''?
Not necessarily…True if G is **abelian**, otherwise not clear.

If **gH=Hg**, then gh=h'g, and the set {gH, g in G} is **closed** under the binary operation.

This does NOT mean gh=hg, this means gh=h'g.

Now suppose we have $(G, \cdot)$ a group, H a normal subgroup of G, i.e., $H \lhd G$, and the set of cosets of H in G, i.e., the set G/H defined by $G/H = \{gH | g \in H\}$.

Theorem 16. *If* $H \lhd G$, *then* $(G/H, (g_1H)(g_2H) = (g_1g_2)H)$ *is a group.*

Proof. To check what we have a group, we verify the definition.

1. Closure: $(g_1H)(g_2H) = g_1(Hg_2)H = g_1g_2H \in G/H$ using that $g_2H = Hg_2$.
2. Associativity follows from that of G.
3. $eH = H$ is the identity in G/H.
4. Finally $g^{-1}H$ is the inverse of gH in G/H, since

$$(gH)(g^{-1}H) = (gg^{-1})H = H.$$

We also need to show that the operation combining two cosets to yield a new coset is well defined. Notice that

$$(gH, g'H) \mapsto gg'H$$

involves the choice of g and g' as representatives. Suppose that we take $g_1 \in gH$ and $g_2 \in g'H$, we need to show that

$$(g_1H, g_2H) \mapsto gg'H.$$

Since $g_1 \in gH$, then $g_1 = gh$ for some h, and similarly, since $g_2 \in g'H$, then $g_2 = g'h'$ for some h' in H, so that

$$g_1H = ghH = gH, \;\; g_2H = g'h'H = g'H$$

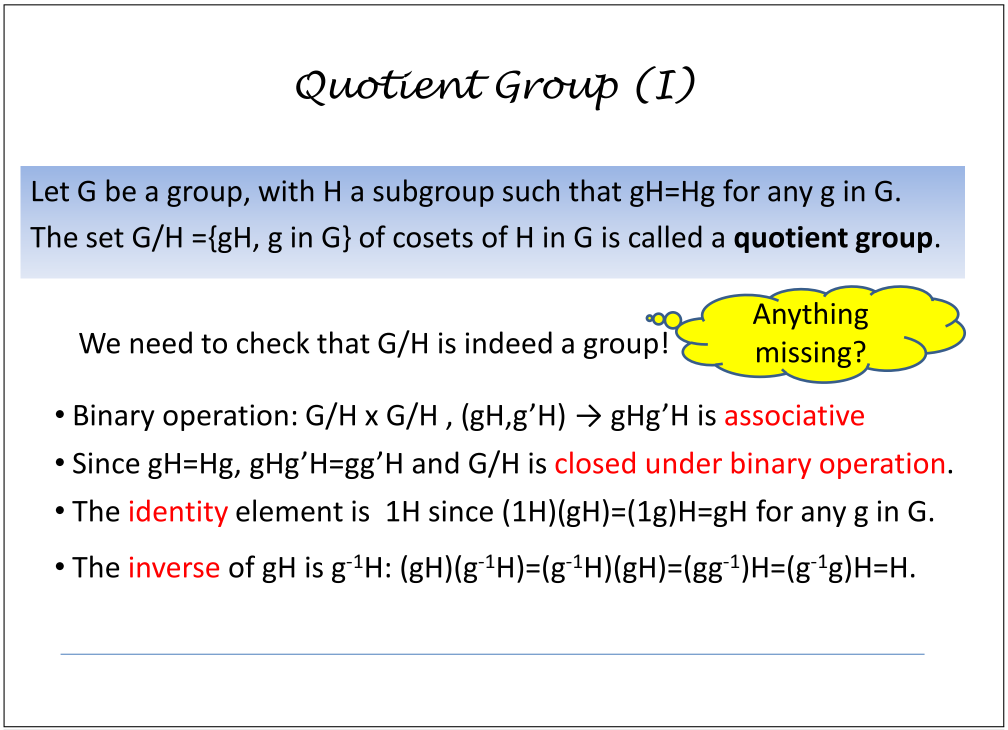
and

$$(g_1H)(g_2H) = (gH)(g'H) = gg'H$$

as desired.

□

The group G/H is called quotient group.



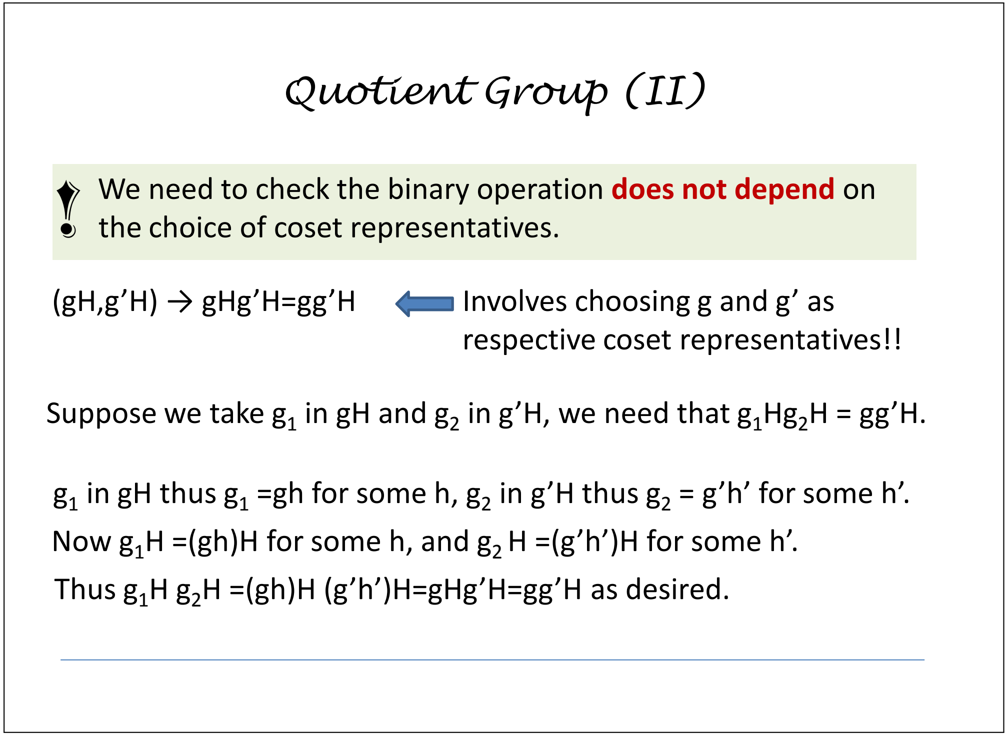
Quotient Group (I)

Let G be a group, with H a subgroup such that gH=Hg for any g in G.
The set G/H ={gH, g in G} of cosets of H in G is called a **quotient group**.

We need to check that G/H is indeed a group!

Anything missing?

- Binary operation: G/H x G/H , (gH,g'H) → gHg'H is associative
- Since gH=Hg, gHg'H=gg'H and G/H is closed under binary operation.
- The identity element is 1H since (1H)(gH)=(1g)H=gH for any g in G.
- The inverse of gH is g^{-1}H: (gH)(g^{-1}H)=(g^{-1}H)(gH)=(gg^{-1})H=(g^{-1}g)H=H.



Quotient Group (II)

! We need to check the binary operation **does not depend** on the choice of coset representatives.

(gH,g'H) → gHg'H=gg'H ⇐ Involves choosing g and g' as respective coset representatives!!

Suppose we take g_1 in gH and g_2 in g'H, we need that g_1Hg_2H = gg'H.

g_1 in gH thus g_1 =gh for some h, g_2 in g'H thus g_2 = g'h' for some h'.
Now g_1H =(gh)H for some h, and g_2 H =(g'h')H for some h'.
Thus g_1H g_2H =(gh)H (g'h')H=gHg'H=gg'H as desired.

The order of the quotient group G/H is given by Lagrange Theorem

$$|G/H| = |G|/|H|.$$

Example 34. Continuing Example 31, where $G = \{0,1,2,3\}$ and $H = \{0,2\}$, we have

$$|G/H| = 4/2 = 2$$

and G/H is isomorphic to C_2.

Example 35. When $G = \mathbb{Z}$, and $H = n\mathbb{Z}$, we cannot use Lagrange since both orders are infinite, still $|G/H| = n$.

Example 36. Consider Dihedral group D_n. The subgroup $H = \langle r \rangle$ of rotations is normal since

1. if r' is any rotation, then $r'r = rr'$,
2. if m is any reflection $\in D_n$, $mr = r^{-1}m$ always.

Hence $rH = Hr$, $mH = Hm$ and $r^i m^j H = r^i H m^j = H r^i m^j$ for $j = 0, 1$ and $i = 0, \ldots, n-1$.

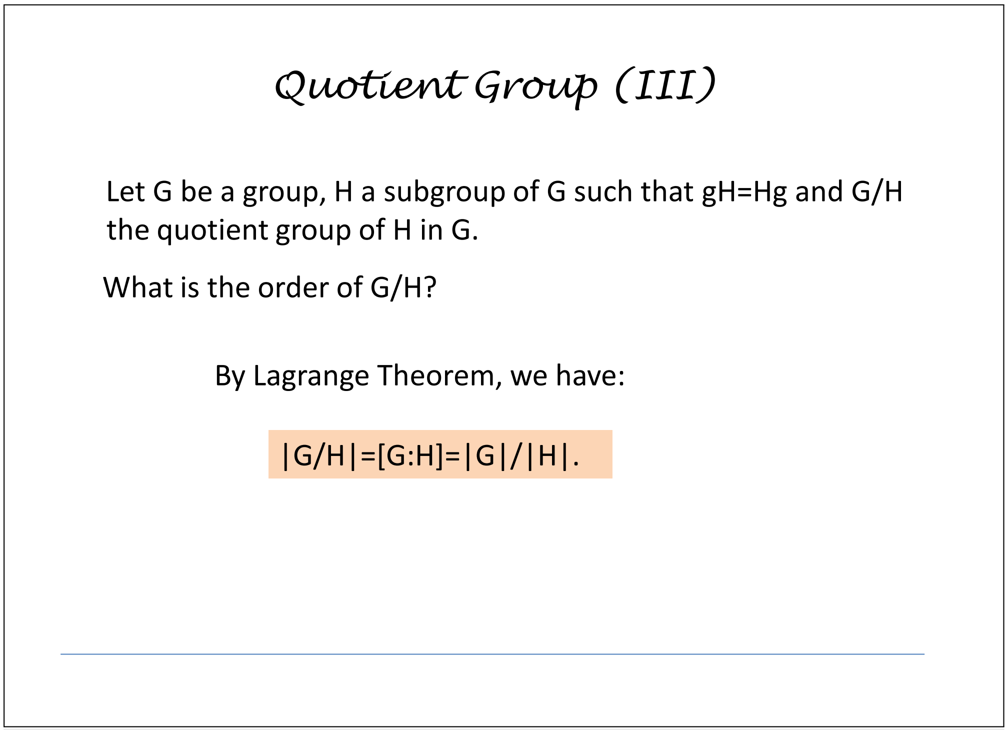
Suppose now G is a cyclic group. Let H be a subgroup of G. We know that H is cyclic as well! Since G is cyclic, it is Abelian, and thus H is normal, showing that G/H is a group! What is this quotient group G/H?

Proposition 10. *The quotient of a cyclic group G is cyclic.*

Proof. Let H be a subgroup of G. Let xH be an element of G/H. To show that G/H is cyclic, we need to show that $xH = (gH)^k$ for some k and gH. Since G is cyclic, $G = \langle g \rangle$ and $x = g^k$ for some k. Thus

$$xH = g^k H = (gH)^k.$$

□



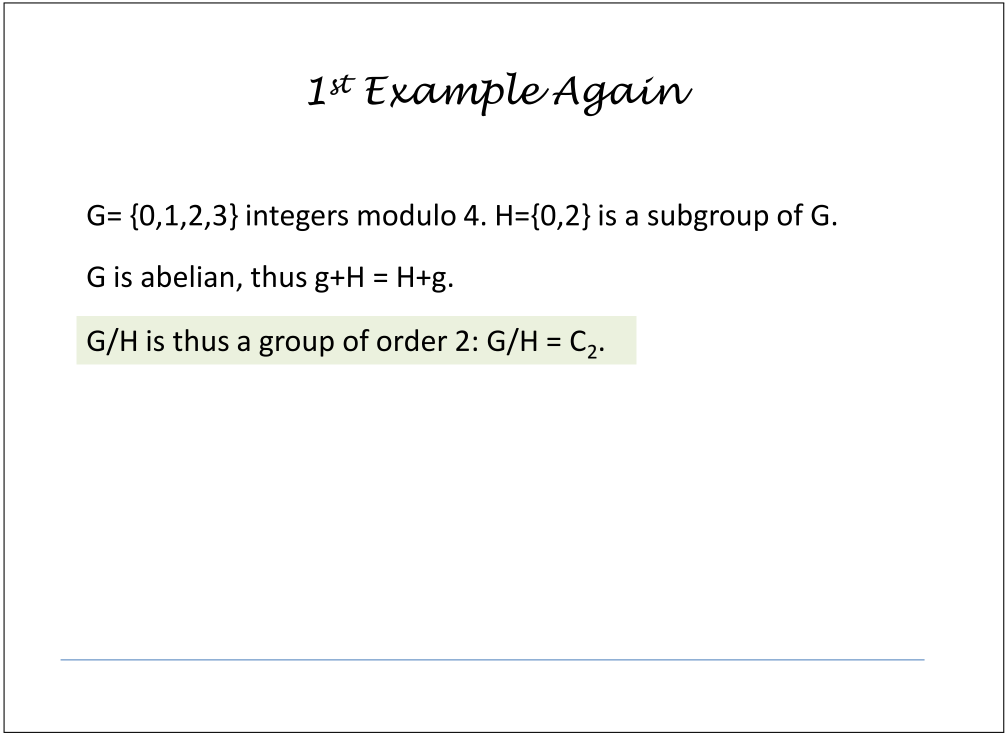
Quotient Group (III)

Let G be a group, H a subgroup of G such that gH=Hg and G/H the quotient group of H in G.

What is the order of G/H?

By Lagrange Theorem, we have:

|G/H|=[G:H]=|G|/|H|.



1^{st} Example Again

G= {0,1,2,3} integers modulo 4. H={0,2} is a subgroup of G.

G is abelian, thus g+H = H+g.

G/H is thus a group of order 2: G/H = C_2.

2^{nd} Example Again

Consider the group G of integers $\mathbb{Z}$. Let H =n$\mathbb{Z}$ be the subgroup formed by multiple of n.

Since $\mathbb{Z}$ is abelian, g+H = H+g for every g in G.

G/H is thus a group of order n.

Here not from Lagrange since the order is infinite!

3^{rd} Example: the Dihedral Group (I)

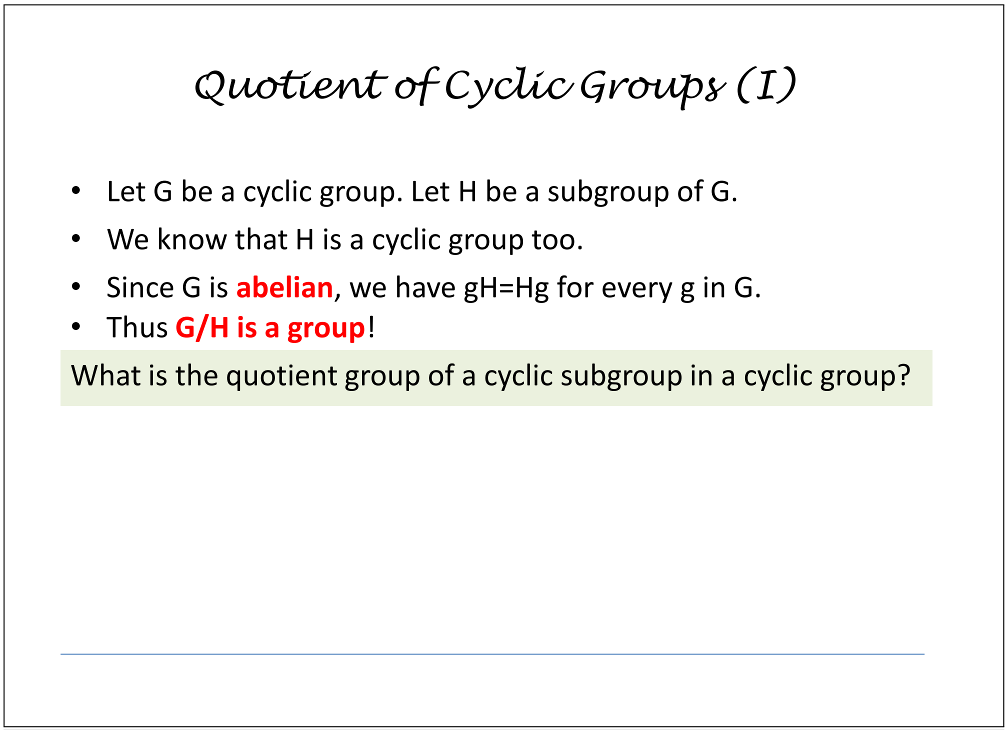
$D_n = \{ <r,m> \mid m^2=1, r^n=1, mr = r^{-1}m \}$

Let r’ be a rotation.

- rr’=r’r since the group of rotations is abelian.
- $mr' = (r')^{-1}m$

➡ H=<r>=group of rotations, then rH=Hr and mH=Hm.

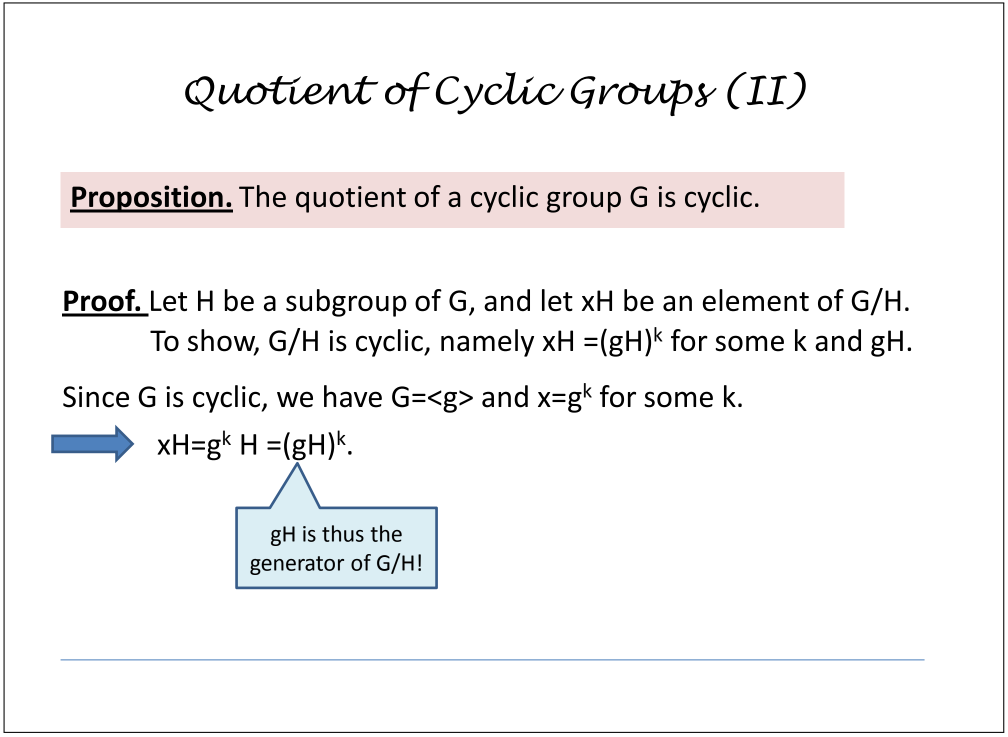
➡ $r^i m^j H = r^i H m^j = H r^i m^j$ for j=0,1 and i=0,…,n-1.



Quotient of Cyclic Groups (I)

- Let G be a cyclic group. Let H be a subgroup of G.
- We know that H is a cyclic group too.
- Since G is **abelian**, we have gH=Hg for every g in G.
- Thus **G/H is a group**!

What is the quotient group of a cyclic subgroup in a cyclic group?



Quotient of Cyclic Groups (II)

Proposition. The quotient of a cyclic group G is cyclic.

Proof. Let H be a subgroup of G, and let xH be an element of G/H. To show, G/H is cyclic, namely $xH=(gH)^k$ for some k and gH.

Since G is cyclic, we have G=<g> and $x=g^k$ for some k.

➡ $xH=g^k H=(gH)^k$.

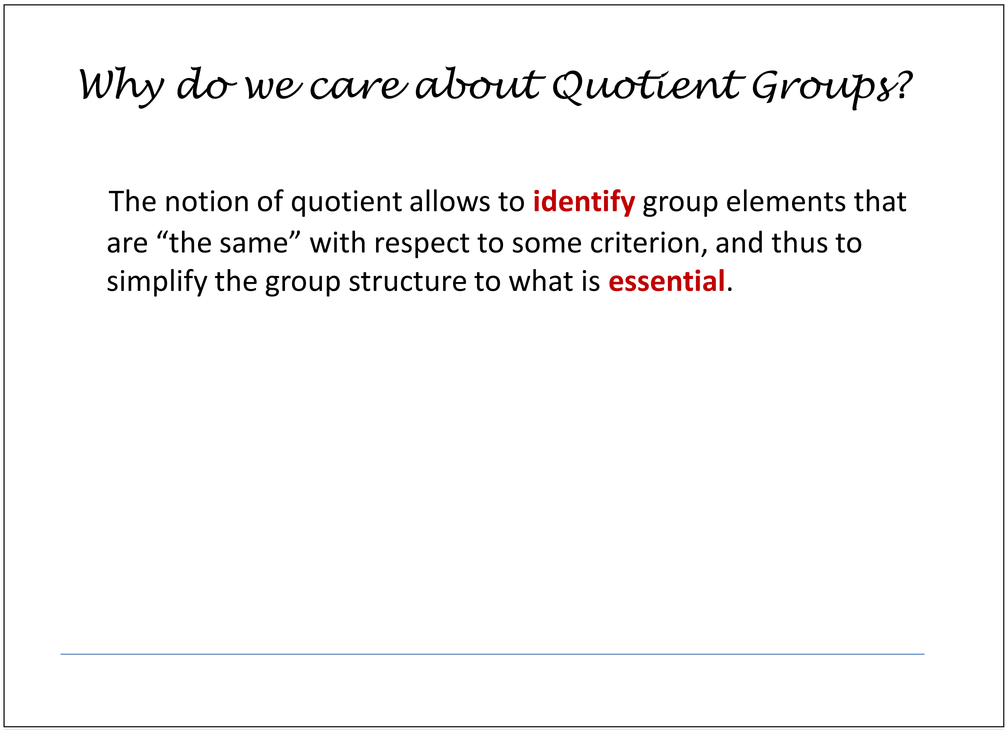
gH is thus the generator of G/H!

The notion of quotient is very important in abstract algebra, since it allows us to simplify a group structure to what is essential!

Example 37. The reals under addition $(\mathbb{R},+)$, the subgroup $(\mathbb{Z},+)$ of integers. We have $(\mathbb{Z},+) \lhd (\mathbb{R},+)$ because of the fact that $(\mathbb{R},+)$ is abelian! Now

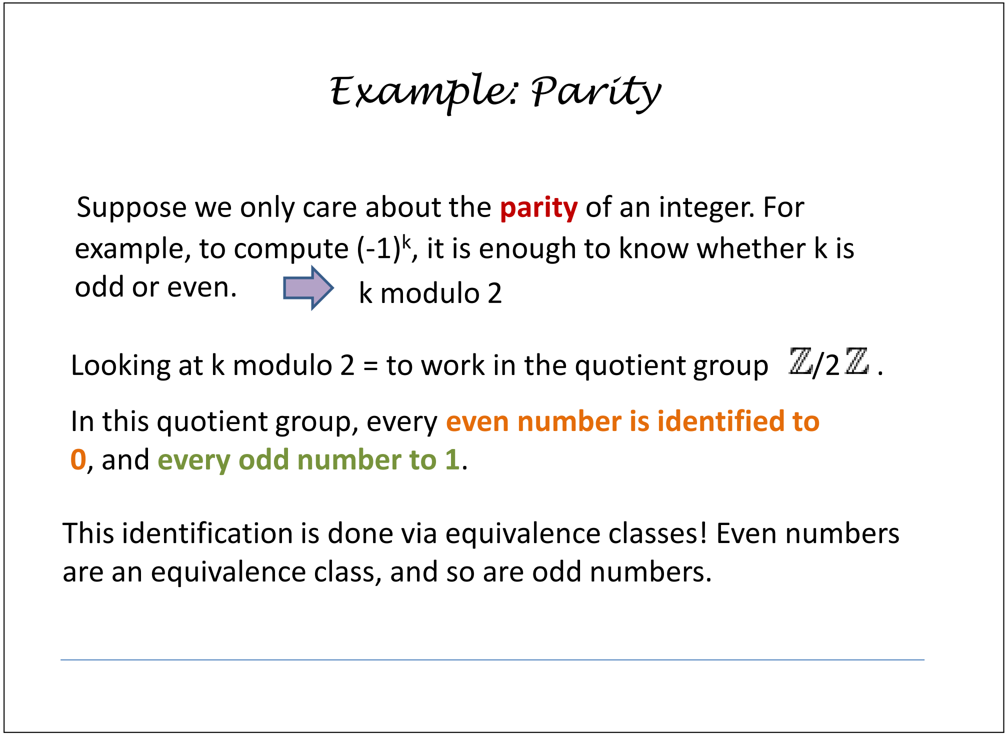
$$\mathbb{R}/\mathbb{Z} = \{r + \mathbb{Z} | r \in \mathbb{R}\}\,.$$

The cosets are $r+\mathbb{Z}$ with $r \in [0,1)$. $\mathbb{R}/\mathbb{Z}$ is isomorphic to the circle group S of complex numbers of absolute value 1. The isomorphism is $\phi[(r+\mathbb{Z})] = e^{i2\pi r}$.



Why do we care about Quotient Groups?

The notion of quotient allows to **identify** group elements that are “the same” with respect to some criterion, and thus to simplify the group structure to what is **essential**.



Example: Parity

Suppose we only care about the **parity** of an integer. For example, to compute $(-1)^k$, it is enough to know whether k is odd or even. ⇒ k modulo 2

Looking at k modulo 2 = to work in the quotient group $\mathbb{Z}/2\mathbb{Z}$.

In this quotient group, every **even number is identified to 0**, and **every odd number to 1**.

This identification is done via equivalence classes! Even numbers are an equivalence class, and so are odd numbers.

Recall Cosets

Recall We have $g_1H=g_2H$ if and only if $g_1^{-1}g_2$ is in H.

Generating the same coset is an equivalence relation!

- It is reflexive: $g^{-1}g=1$ is in H
- It is symmetric: if $g_1^{-1}g_2$ is in H, then $(g_1^{-1}g_2)^{-1}=g_2^{-1}g_1$ is in H.
- It is transitive: if $g_1^{-1}g_2$ in H and $g_2^{-1}g_3$, then $(g_1^{-1}g_2)(g_2^{-1}g_3)=g_1^{-1}g_3$ in H.

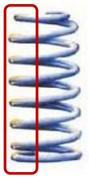
⇨ a coset = an equivalence class

group elements that are "the same" with respect to some criterion

One more Example (I)

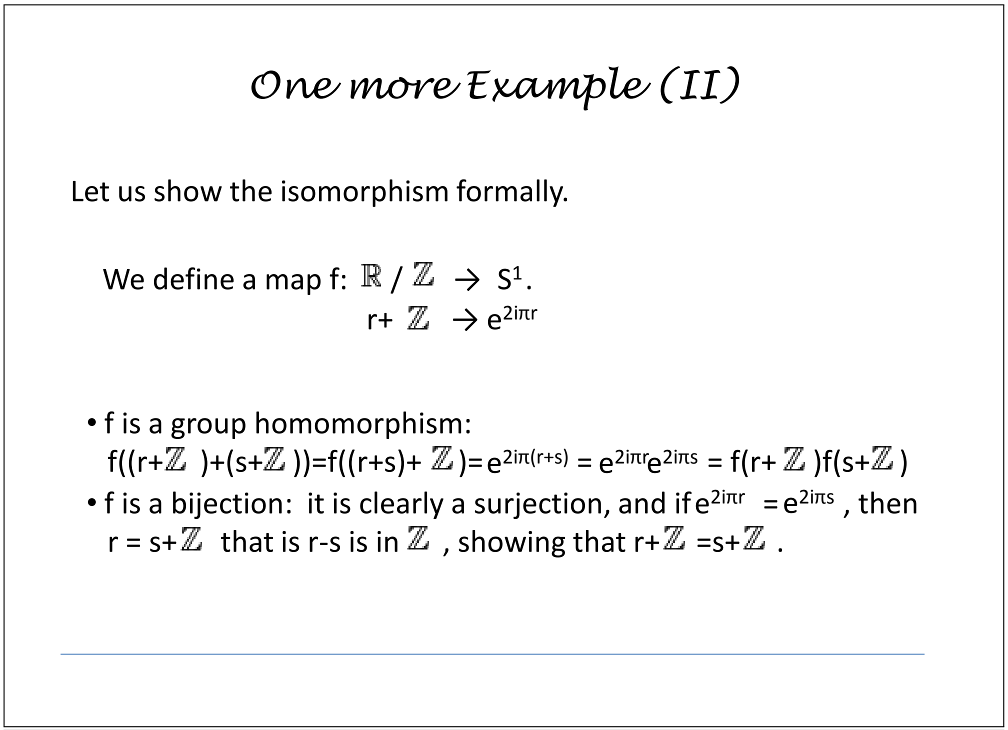
Take G=($\mathbb{R}$,+), it has H=($\mathbb{Z}$,+) as a subgroup. Since G is abelian, we have that $g+\mathbb{Z}=\mathbb{Z}+g$.

What is the quotient group G/H ?



G/H = S^1 (circle)

1.http://www.dreamteamcar.fr/upload/RessortOMEAJ2.jpg

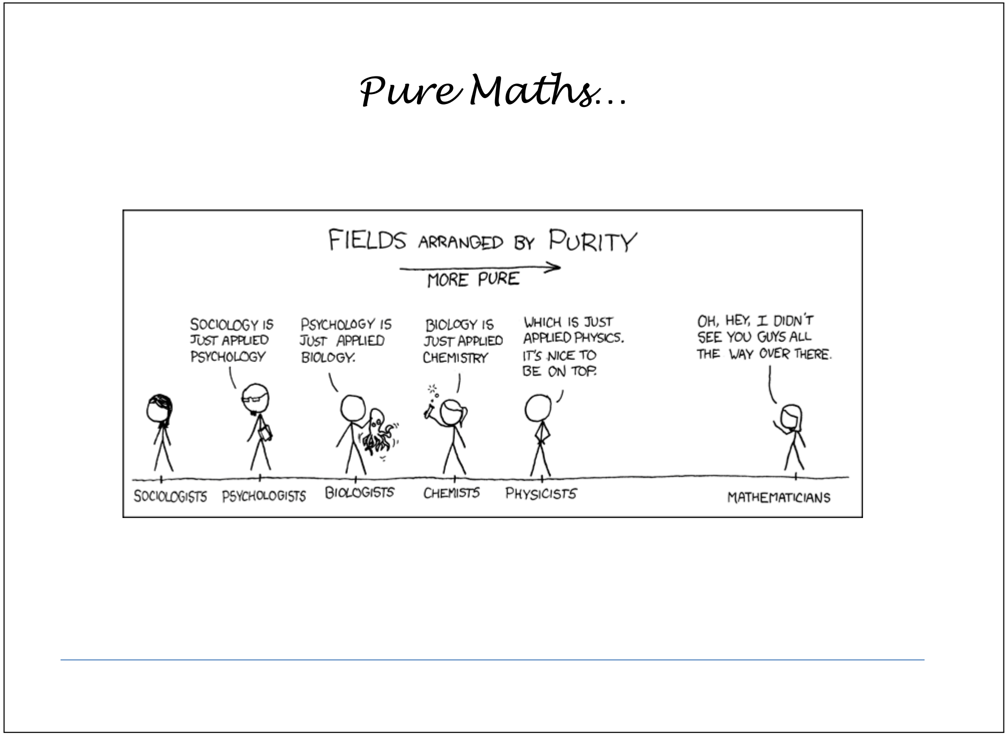


One more Example (II)

Let us show the isomorphism formally.

We define a map f: $\mathbb{R} / \mathbb{Z} \to S^1$.
$r+\mathbb{Z} \to e^{2i\pi r}$

- f is a group homomorphism:
  $f((r+\mathbb{Z})+(s+\mathbb{Z}))=f((r+s)+\mathbb{Z})=e^{2i\pi(r+s)} = e^{2i\pi r}e^{2i\pi s} = f(r+\mathbb{Z})f(s+\mathbb{Z})$
- f is a bijection: it is clearly a surjection, and if $e^{2i\pi r} = e^{2i\pi s}$, then $r = s+\mathbb{Z}$ that is r-s is in $\mathbb{Z}$, showing that $r+\mathbb{Z} = s+\mathbb{Z}$.



Pure Maths…

FIELDS ARRANGED BY PURITY
MORE PURE
SOCIOLOGY IS JUST APPLIED PSYCHOLOGY
PSYCHOLOGY IS JUST APPLIED BIOLOGY.
BIOLOGY IS JUST APPLIED CHEMISTRY
WHICH IS JUST APPLIED PHYSICS. IT'S NICE TO BE ON TOP.
OH, HEY, I DIDN'T SEE YOU GUYS ALL THE WAY OVER THERE.
SOCIOLOGISTS
PSYCHOLOGISTS
BIOLOGISTS
CHEMISTS
PHYSICISTS
MATHEMATICIANS

Exercises for Chapter 9

Exercise 43. Consider the Klein group $G = \{1, f, g, h\}$.

- What are all the possible subgroups of G?
- Compute all the possible quotient groups of G.

Exercise 44. Consider the dihedral group D_4. What are all the possible quotient groups of D_4?

Exercise 45. Consider A the set of affine maps of $\mathbb{R}$, that is

$$A = \{f : x \mapsto ax + b,\ a \in \mathbb{R}^*,\ b \in \mathbb{R}\}.$$

1. Show that A is a group with respect to the composition of maps.
2. Let
$$N = \{g : x \mapsto x + b,\ b \in \mathbb{R}\}.$$
Show that the set of cosets of N forms a group.
3. Show that the quotient group A/N is isomorphic to $\mathbb{R}^*$.

Chapter 10

Infinite Groups

The groups we have carefully studied so far are finite groups. In this chapter, we will give a few examples of infinite groups, and revise some of the concepts we have seen in that context.

Let us recall a few examples of infinite groups we have seen:

- the group of real numbers (with addition),
- the group of complex numbers (with addition),
- the group of rational numbers (with addition).

Instead of the real numbers $\mathbb{R}$, we can consider the real plane $\mathbb{R}^2$. Vectors in $\mathbb{R}^2$ form a group structure as well, with respect to addition! Let us check that this is true. For that, we check our 4 usual properties: (1) the sum of two vectors is a vector (closure), (2) addition of vectors is associative, (3) there is an identity element, the vector $(0, 0)$, and (4) every vector $(x_1, x_2) \in \mathbb{R}^2$ has an inverse, given by $(-x_1, -x_2)$, since

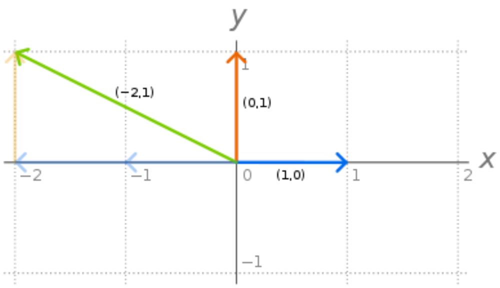
$$(x_1, x_2) + (-x_1, -x_2) = (0, 0).$$

Examples of Infinite Groups

- The real numbers
- The complex numbers
- The rational numbers

Anything else?

The 2-dimensional Real Plane



http://upload.wikimedia.org/wikipedia/commons/thumb/9/9a/Basis_graph_%28no_label%29.svg/400px-Basis_graph_%28no_label%29.svg.png

The example that we just saw with $\mathbb{R}^2$ is a special case of a vector space. Vector spaces are objects that you might have seen in a linear algebra course. Let us recall the definition of a vector space.

Definition 19. A set V is a vector space over a field (for us, we can take this field to be $\mathbb{R}$) if for all $u, v, w \in V$

1. $u + v \in V$ (closure property),
2. $u + v = v + u$ (commutativity),
3. $u + (v + w) = (u + v) + w$ (associativity),
4. there exists $0 \in V$ such that $u + 0 = 0 + u$,
5. there exists $-v$ such that $(-v) + v = 0$

and for all $x, y \in \mathbb{R}$ we have

1. $x(u + v) = xu + xv$,
2. $(x + y)u = xu + xu$,
3. $x(yu) = (xy)u$
4. $1u = u$, where 1 is the identity of $\mathbb{R}$.

We recognize that the first axioms of a vector space V are in fact requesting V to be an Abelian group!

Example 38. The n-dimensional real space $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n)\,|x_i \in \mathbb{R},\ i = 1, \dots, n\}$ is a vector space over the reals.

Example 39. We already know that the set $\mathbb{C}$ of complex numbers forms a group. Now

$$\mathbb{C} = \{x + iy|x, y \in \mathbb{R}\}$$

is a vector space over $\mathbb{R}$, which gives another proof that $\mathbb{C}$ forms a group under addition.

Definition of Vector Space

A set V of vectors, a set F (field, say the real numbers) of scalars.

- **Associativity** of vector addition: $\mathbf{v_1} + (\mathbf{v_2} + \mathbf{v_3}) = (\mathbf{v_1} + \mathbf{v_2}) + \mathbf{v_3}$.
- **Commutativity** of vector addition: $\mathbf{v_1} + \mathbf{v_2} = \mathbf{v_2} + \mathbf{v_1}$.
- **Identity element** of vector addition: there exists $\mathbf{0} \in V$ such that $\mathbf{v} + \mathbf{0} = \mathbf{v}$ for all $\mathbf{v} \in V$.
- **Inverse elements** of vector addition: for all $\mathbf{v} \in$ V, there exists $\mathbf{-v} \in V$ such that $\mathbf{v} + \mathbf{(-v)} = \mathbf{0}$.
- **Distributivity** of scalar multiplication w/r vector addition: $n(\mathbf{v_1} + \mathbf{v_2}) = n\mathbf{v_1} + n\mathbf{v_2}$.
- **Distributivity** of scalar multiplication w/r field addition : $(n_1 + n_2)\mathbf{v} = n_1\mathbf{v} + n_2\mathbf{v}$.
- Respect of scalar multiplication over field multiplication: $n_1 (n_2 \mathbf{v}) = (n_1 n_2)\mathbf{v}$.
- Identity element of scalar multiplication: $1\mathbf{v} = \mathbf{v}$, where 1 = multiplicative identity in *F*.

We recognize the group definition!

Definition of Vector Space Revisited

The word field can be easily replaced by real numbers if you don't know it.

A set V of vectors, a set F (field, say the real numbers) of scalars.

- **Vectors form an abelian group with respect to addition.**
- **Inverse elements** of vector addition: for all $\mathbf{v} \in$ V, there exists $\mathbf{-v} \in V$ such that $\mathbf{v} + \mathbf{(-v)} = \mathbf{0}$.
- **Distributivity** of scalar multiplication w/r vector addition: $s(\mathbf{v_1} + \mathbf{v_2}) = s\mathbf{v_1} + s\mathbf{v_2}$.
- **Distributivity** of scalar multiplication w/r field addition : $(n_1 + n_2)\mathbf{v} = n_1\mathbf{v} + n_2\mathbf{v}$.
- Respect of scalar multiplication over field multiplication: $n_1 (n_2 \mathbf{s}) = (n_1 n_2)\mathbf{s}$.
- Identity element of scalar multiplication: $1\mathbf{s} = \mathbf{s}$, where 1 = multiplicative identity in *F*.

A vector space is thus an Abelian group. What is the order of this group? It's infinity!

Now we might wonder what are the subgroups of this group. They are in fact subspaces, as follows from the definition of a subspace.

Definition 20. Let V be a vector space over some field F and U be a subset of V. If U is a vector space over F under the operations of V (vector addition and multiplication by elements of F), then U is called a subspace of V.

Let us recall the definition of a basis of a vector space.

Definition 21. A basis of V is a set of **linearly independent** vectors of V such that every element v is a linear combination of the vectors from this set.

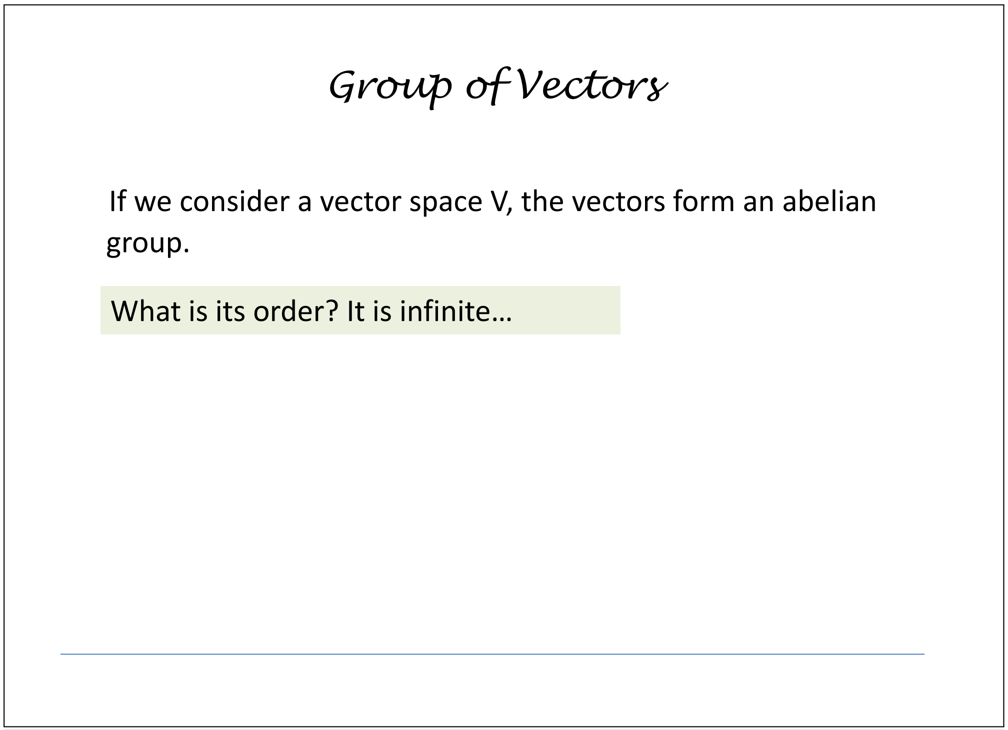
Example 40. The set $\{(1,0),(0,1)\}$ is a basis of the two-dimensional plane $\mathbb{R}^2$. This means that every vector $x \in \mathbb{R}^2$ can be written as

$$x = x_1(1,0) + x_2(0,1),\ x_1, x_2 \in \mathbb{R}.$$

Now let us think of what happens in the above example if we keep the two basis vectors $(1,0)$ and $(0,1)$, but now restrict to integer coefficients x_1, x_2. We get a set of the form

$$\{x = x_1(1,0) + x_2(0,1),\ x_1, x_2 \in \mathbb{Z}\}.$$

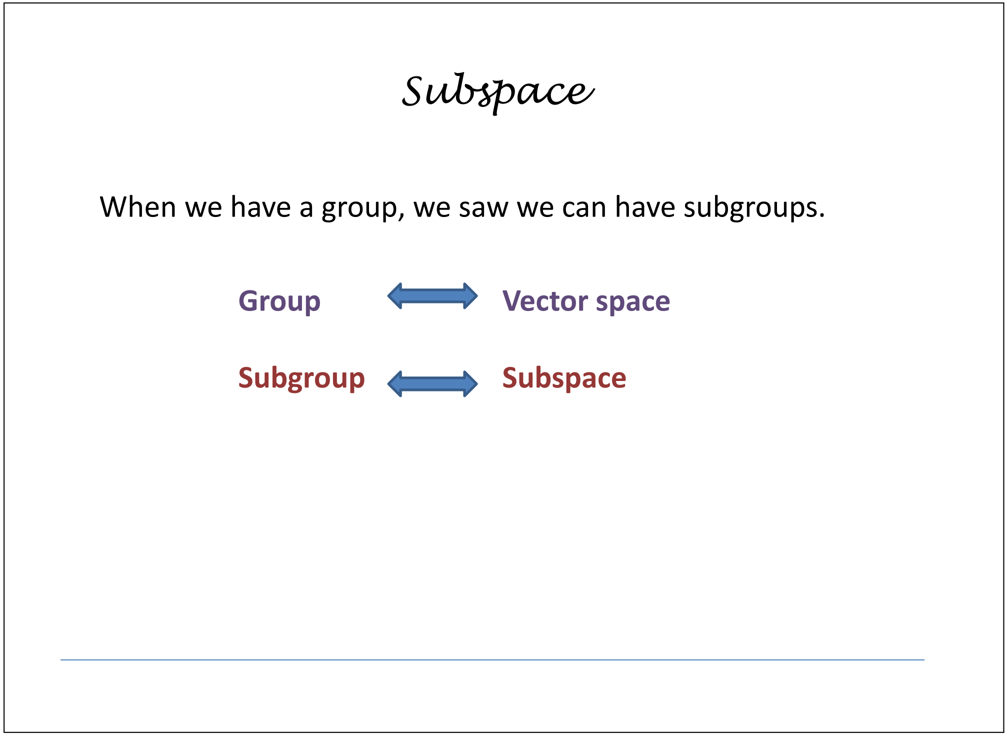
If you plot it, you will see that you find an integer grid!



Group of Vectors

If we consider a vector space V, the vectors form an abelian group.

What is its order? It is infinite…



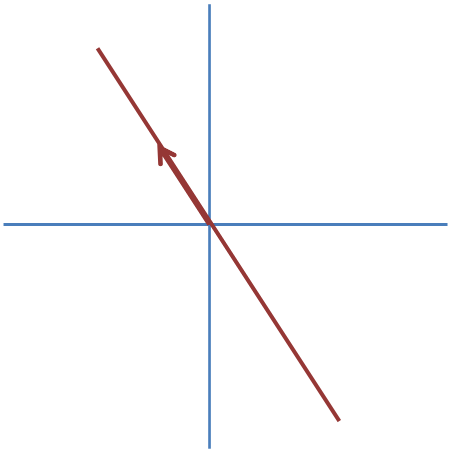
Subspace

When we have a group, we saw we can have subgroups.

Group ⟺ **Vector space**

Subgroup ⟺ **Subspace**

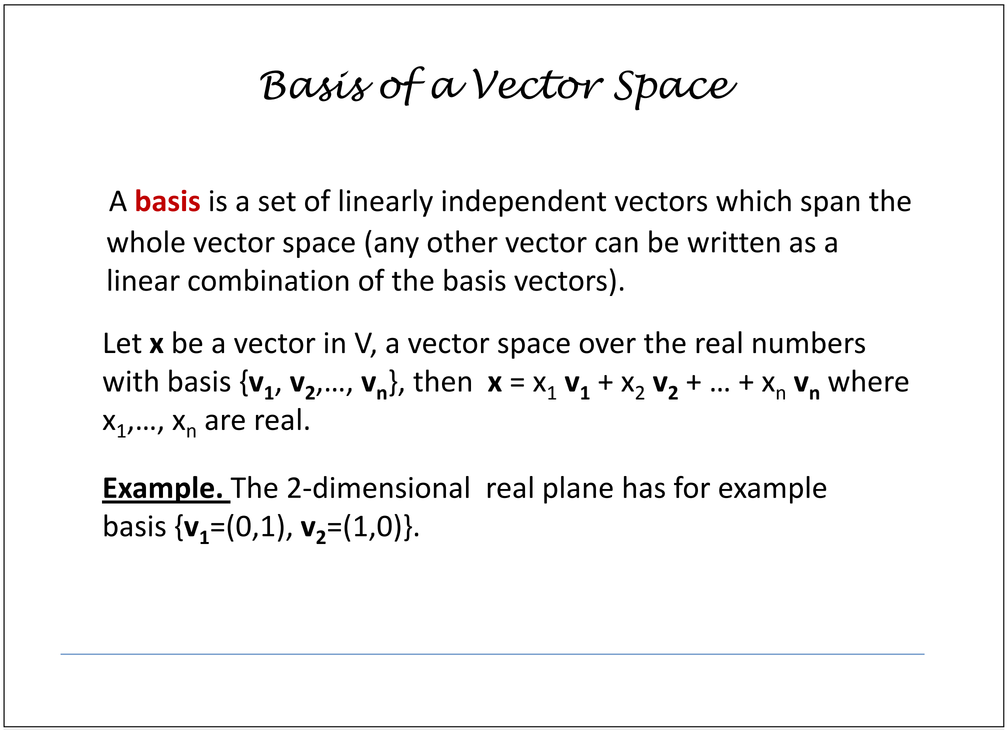
Subspaces of the 2-dimensional Plane



Subspace

A subset of a vector space which is also a vector space is called a **subspace**.

A subspace of V is thus a **subgroup** of the group V of vectors.

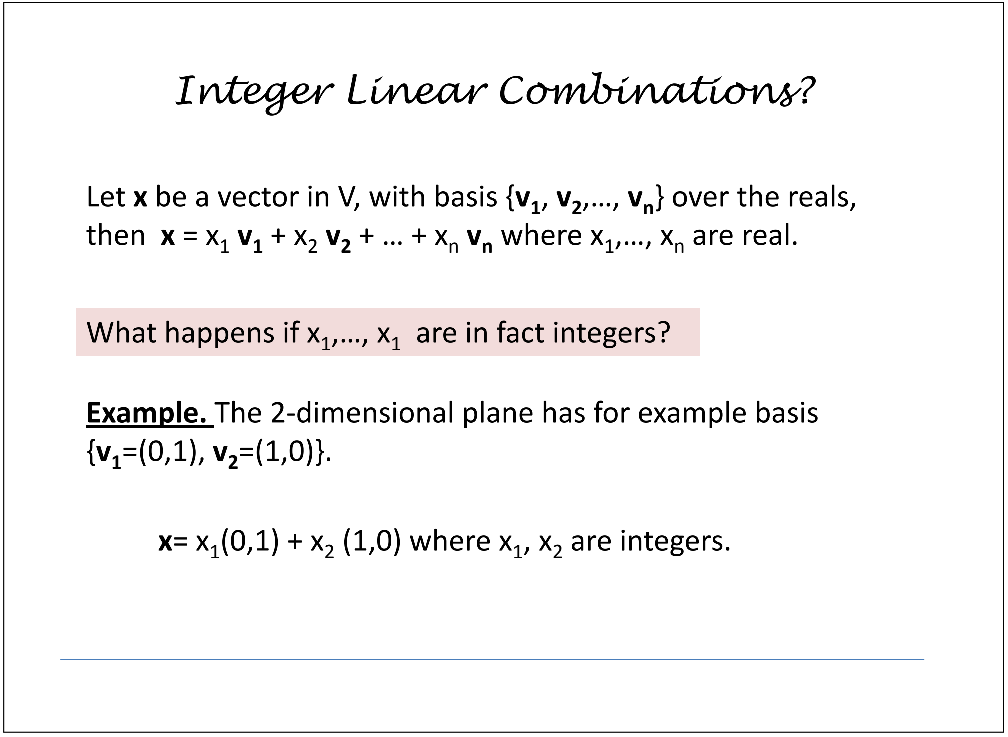


Basis of a Vector Space

A **basis** is a set of linearly independent vectors which span the whole vector space (any other vector can be written as a linear combination of the basis vectors).

Let $\mathbf{x}$ be a vector in V, a vector space over the real numbers with basis $\{\mathbf{v_1}, \mathbf{v_2},\dots, \mathbf{v_n}\}$, then $\mathbf{x} = x_1 \mathbf{v_1} + x_2 \mathbf{v_2} + \dots + x_n \mathbf{v_n}$ where $x_1,\dots, x_n$ are real.

Example. The 2-dimensional real plane has for example basis $\{\mathbf{v_1}=(0,1), \mathbf{v_2}=(1,0)\}$.



Integer Linear Combinations?

Let $\mathbf{x}$ be a vector in V, with basis $\{\mathbf{v_1}, \mathbf{v_2},\dots, \mathbf{v_n}\}$ over the reals, then $\mathbf{x} = x_1 \mathbf{v_1} + x_2 \mathbf{v_2} + \dots + x_n \mathbf{v_n}$ where $x_1,\dots, x_n$ are real.

What happens if $x_1,\dots, x_1$ are in fact integers?

Example. The 2-dimensional plane has for example basis $\{\mathbf{v_1}=(0,1), \mathbf{v_2}=(1,0)\}$.

$\mathbf{x}= x_1(0,1) + x_2 (1,0)$ where x_1, x_2 are integers.

We might ask whether the integer grid

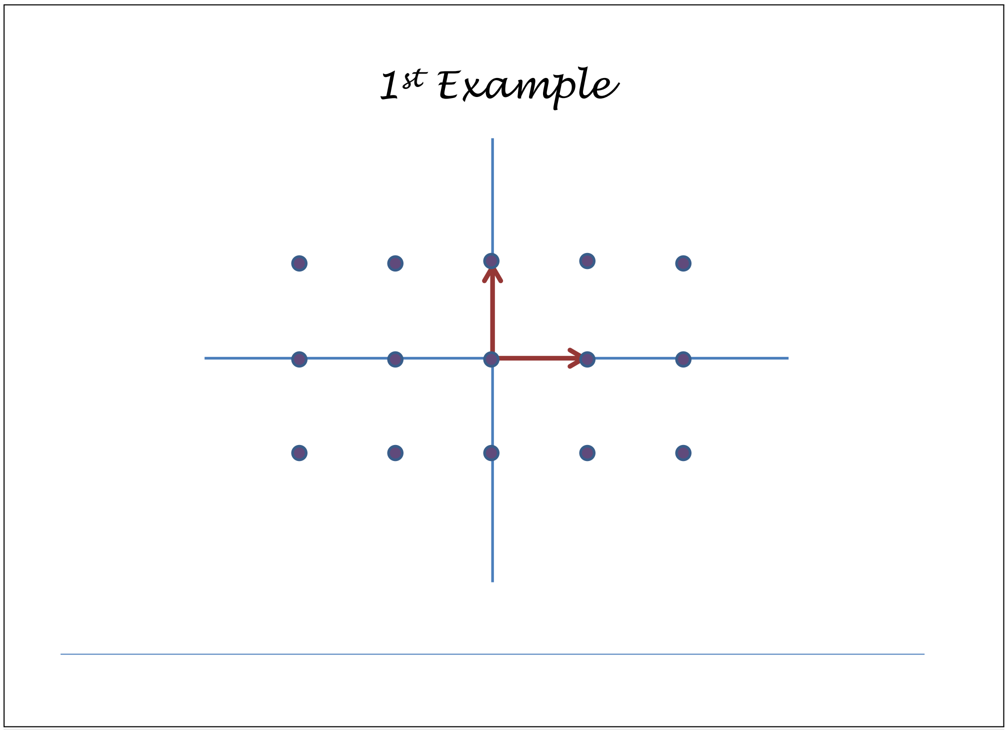
$$\{x = x_1(1,0) + x_2(0,1),\ x_1, x_2 \in \mathbb{Z}\}$$

still has a group structure. In fact, we could ask the same question more generally. Suppose that we have two linearly independent vectors v_1, v_2, does the set

$$L = \{x = x_1 v_1 + x_2 v_2,\ x_1, x_2 \in \mathbb{Z}\}$$

form a group? We already know that addition of vectors is associative. If we take two vectors in L, their sum still is a vector in L (we need to make sure that the coefficients still are integers), so the closure property is satisfied. The identity element is the vector $(0,0)$, and every element has an inverse. Indeed, if we have a vector (x_1, x_2) with integer coefficients then $(-x_1, -x_2)$ also has integer coefficients, and their sum is $(0,0)$. In that case, L is called a lattice, and it forms an infinite Abelian group.

A subset of the lattice L which itself has a subgroup structure is called a sublattice.



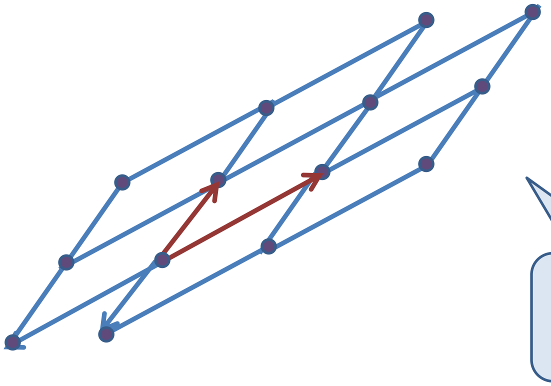
1^{st} Example

Group Structure?

Take two linearly independent vectors $\mathbf{v_1}$,$\mathbf{v_2}$ in the 2-dimensional real plane. Consider the set $\{x_1\mathbf{v_1}+x_2\mathbf{v_2}, x_1,x_2 \text{ integers}\}$.

Does it form a group?

2nd Example



This forms an infinite group!

Lattice

Take two linearly independent vectors $\mathbf{v_1},\mathbf{v_2}$ in the 2-dimensional real plane. The set $L=\{x_1\mathbf{v_1}+x_2\mathbf{v_2}, x_1,x_2$ integers$\}$ forms a **group** called a **lattice**.

- Addition of vectors is associative.
- Closure: $(x_1\mathbf{v_1}+x_2\mathbf{v_2})+(x_3\mathbf{v_1}+x_4\mathbf{v_2})= (x_1+x_3)\mathbf{v_1}+(x_2+x_4)\mathbf{v_2}$ is in L.
- Inverse: $-x_1\mathbf{v_1}-x_2\mathbf{v_2}$ is the inverse of $x_1\mathbf{v_1}+x_2\mathbf{v_2}$ is in L.
- Identity is the zero vector.

A lattice is an infinite abelian group.

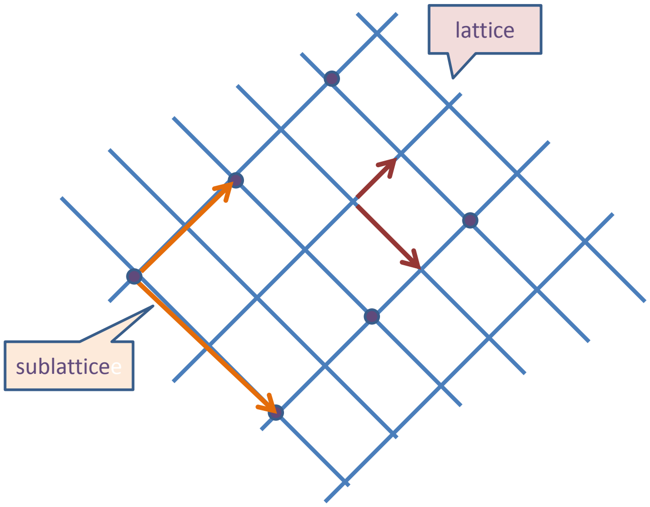
Sublattice

When we have a group, we saw we can have subgroups.

Group ⟺ **Lattice**

Subgroup ⟺ **Sublattice**

3^{rd} Example



We spent quite some time at the beginning of theses lectures to study isometries of the plane. What happens with the isometries of the integer grid?

The isometries of $\mathbb{R}^2 \to \mathbb{R}^2$ were completely characterized and analyzed before and we know that a planar isometry φ is of the form

$$\begin{aligned} \varphi \quad &: \quad (x,y) \mapsto (x',y') \\ \begin{bmatrix} x' \\ y' \end{bmatrix} \quad &= \quad \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & (-1)^{\varepsilon} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}. \end{aligned}$$

Let us now consider the integer grid lattice

$$\mathbb{Z}^2 = \{(m,n) | m \in \mathbb{Z},\, n \in \mathbb{Z}\}.$$

The isometries of the integer lattice, under the Euclidean distance defined over $\mathbb{R}^2$ will be a subgroup of the group of planar isometries, i.e., they will be of the form

$$\begin{aligned} \varphi_D \quad &: \quad (m,n) \mapsto (m',n') \\ \begin{bmatrix} m' \\ n' \end{bmatrix} \quad &= \quad R_{\theta_D} \begin{bmatrix} 1 & 0 \\ 0 & (-1)^{\varepsilon} \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} + \begin{bmatrix} \beta_1 \\ \beta_2 \end{bmatrix}_D. \end{aligned}$$

The restriction of having to map integer coordinate points to integer coordinate points immediately imposes the following constraints on θ_D and $[\beta_1, \beta_2]_D$:

1. $[\beta_1, \beta_2]_D \in \mathbb{Z}^2$
2. $\cos\theta$ and $\sin\theta$ must be integers or zero, hence their possibilities are $\{-1, 0, 1\}$ yielding $\theta = 0, 90°, 180°, 270°, 360°$.

Hence the set of isometries of the integer lattice/grid forms a group of planar transformations involving integer vector translations and rotations by multiples of 90°.

Isometries of the Plane

We already know:

Theorem An isometry H of the plane is necessarily of the form

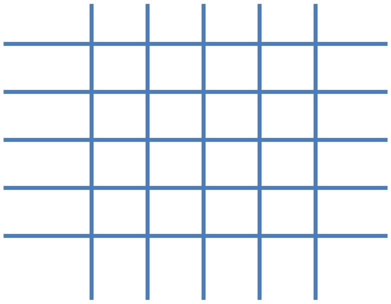
- $H(z)= \alpha z + \beta$, or
- $H(z)=\alpha\bar{z} + \beta$

with $|\alpha|=1$ and some complex number β.

In matrix form:
$R_\theta M \mathbf{z} + \mathbf{b}$, where R_θ =rotation matrix by angle of θ,
M=reflection matrix, **b**=translation vector.

Isometries of the Integer Grid (I)

We keep the basis vectors (1,0) and (0,1), but now instead of the 2-dimensional plane, by taking integer coefficients, we get the integer grid.



Isometries of the Integer Grid (II)

What are the isometries of the integer grid?

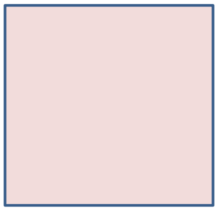
They are a subset (in fact subgroup) of the isometries of the plane, which **sends integer points to integer points.**

In matrix form:
$R_\theta M \mathbf{z} + \mathbf{b}$, where R_θ =rotation matrix by angle of θ,
M=reflection matrix, **b**=translation vector.

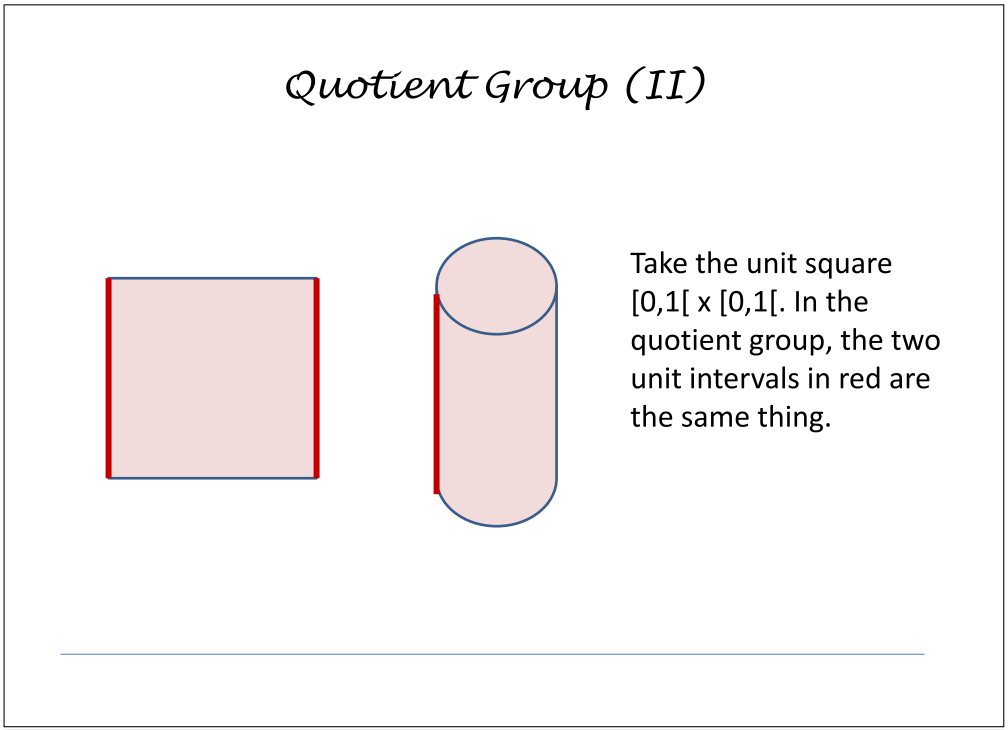
1. The translation vector **b** must be part of the integer grid.
2. cosθ and sinθ must be 0,+1 or -1.

Quotient Group (I)

- The integer grid lattice is a subgroup H of the 2-dimensional real plane seen as an abelian group G.
- Since G is abelian, H satisfies that g+H = H+g.
  What is the quotient group G/H?

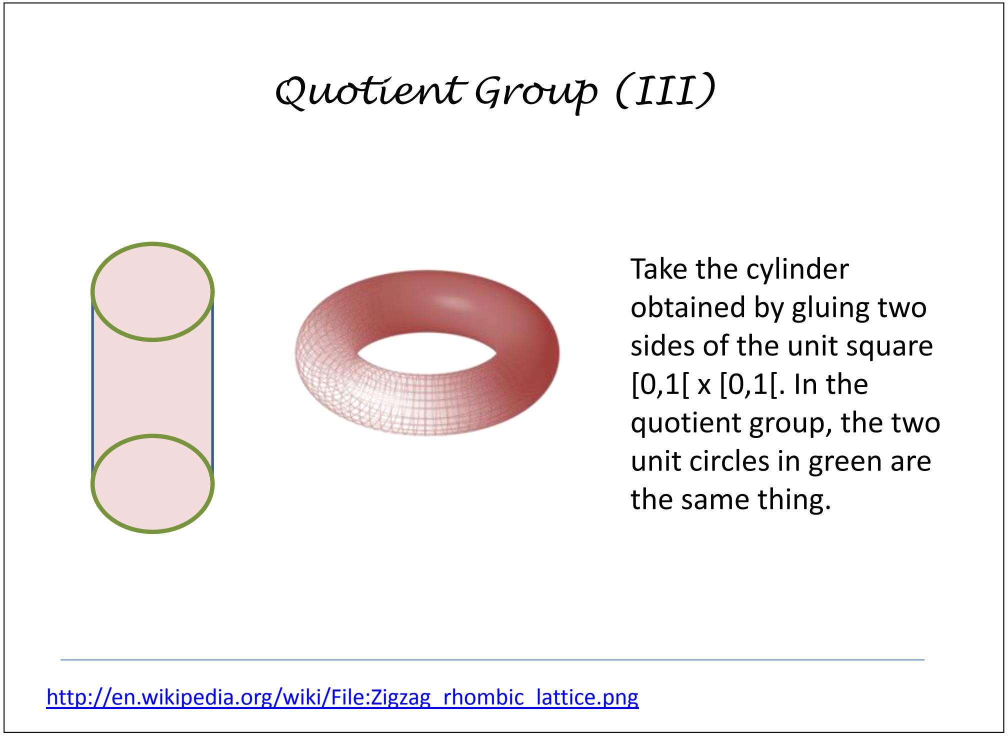


Take the unit square
[0,1[x [0,1[.



Quotient Group (II)

Take the unit square [0,1[x [0,1[. In the quotient group, the two unit intervals in red are the same thing.



Quotient Group (III)

Take the cylinder obtained by gluing two sides of the unit square [0,1[x [0,1[. In the quotient group, the two unit circles in green are the same thing.

http://en.wikipedia.org/wiki/File:Zigzag_rhombic_lattice.png

Exercises for Chapter 10

Exercise 46.

- Show that the complex numbers $\mathbb{C}$ form a vector space over the reals.
- Give a basis of $\mathbb{C}$ over the reals.
- In the lecture, we saw for $\mathbb{R}^2$ that we can obtain a new group, called a lattice, by keeping a basis of $\mathbb{R}^2$ but instead considering integer linear combinations instead of real linear combinations. What happens for $\mathbb{C}$ if we do the same thing? (namely consider integer linear combinations).

Exercise 47. Consider the set $\mathcal{M}_2(\mathbb{R})$ of 2×2 matrices with real coefficients.

1. Show that $\mathcal{M}_2(\mathbb{R})$ forms a vector space over the reals.
2. Deduce that it has an abelian group structure.
3. Give a basis of $\mathcal{M}_2(\mathbb{R})$ over the reals.
4. What happens for $\mathcal{M}_2(\mathbb{R})$ if we keep a basis over the reals and consider only integer linear combinations instead of real linear combinations? Do we also get a new group? If so, describe the group obtained.

Chapter 11

Frieze Groups

We conclude this class by looking at frieze groups. A frieze pattern is a two dimensional image that repeats periodically in one direction. We shall consider that the repetition is in the x-axis direction.

The repetition periodicity will be set to 1. Therefore we are considering a bivariate function $I(x, y)$ periodic in x, that is such that

$$I(x+1, y) = I(x, y),\ \ x \in (-\infty, +\infty)$$

.

Usually y is restricted to $y \in [-\frac{1}{2}, \frac{1}{2}]$, so that the frieze is a unit width band carrying a repetitive pattern in the x-direction. Frieze patterns are popular ornaments in architecture, textiles, on fences etc., and can be very beautiful and elaborate. We will study the possible symmetries that such patterns can have, and we shall prove that there are exactly seven groups of isometries that can arise as symmetries of planar friezes.

By definition, all the symmetry groups of friezes will have the subgroup of translations by integers in the x-direction included. This subgroup is generated by the basic mapping

$$\tau : (x, y) \mapsto (x+1, y).$$

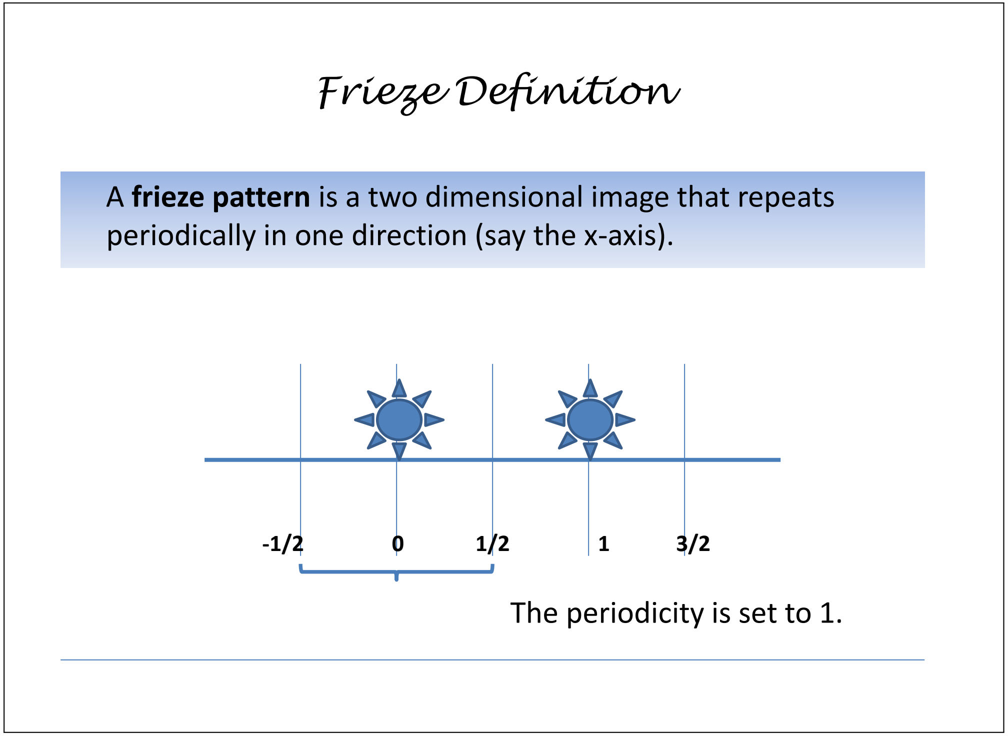
$\langle\tau\rangle$ is the infinite cyclic group of integer translations isomorphic to $(\mathbb{Z}, +)$.

Now the basic pattern of the frieze defined over the square $[-\frac{1}{2}, \frac{1}{2}] \times [-\frac{1}{2}, \frac{1}{2}]$ is a finite planar shape which can have symmetries and properties that may induce further symmetries for the whole frieze.

What are Friezes?

Pottery jar, Southern Iraq (4500-4000 BC).

http://en.wikipedia.org/wiki/File:Frieze-group-3-example1.jpg

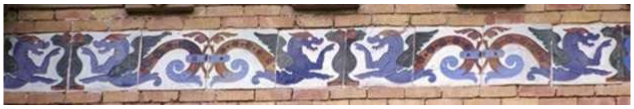


Frieze Definition

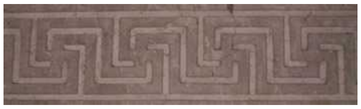
A **frieze pattern** is a two dimensional image that repeats periodically in one direction (say the x-axis).

The periodicity is set to 1.

More Examples



Tile Frieze, Palacio de Velazquez, Madrid, Spain

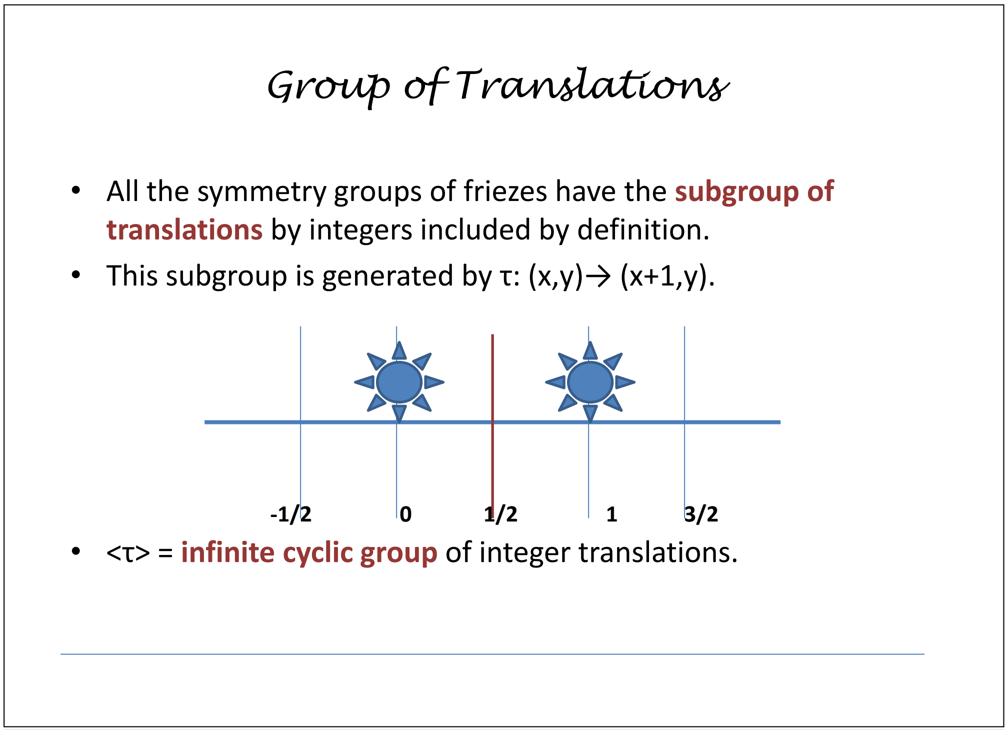


Meander Frieze, San Giorgio Maggiore, Venice, Italy

http://mathdl.maa.org/images/upload_library/4/vol1/architecture/Math/f3.jpg
http://mathdl.maa.org/images/upload_library/4/vol1/architecture/Math/f4.jpg

Frieze Groups

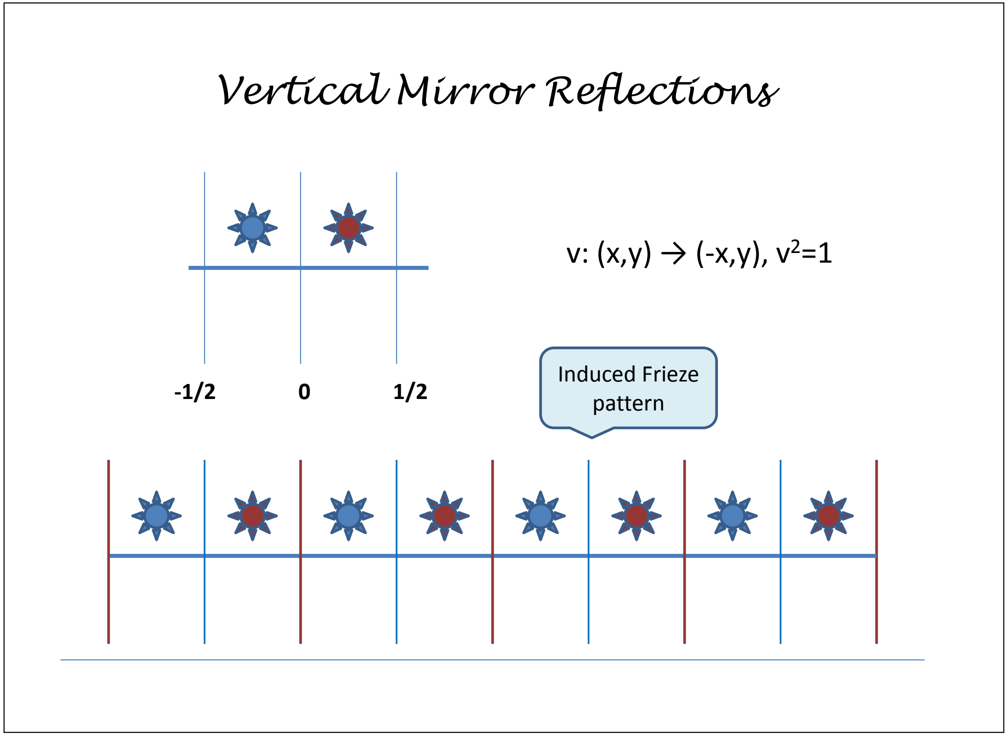
- **Groups of symmetries** of frieze patterns.
- We will see: there are exactly **7** such groups.



Group of Translations

- All the symmetry groups of friezes have the **subgroup of translations** by integers included by definition.
- This subgroup is generated by $\tau: (x,y) \rightarrow (x+1,y)$.

- $<\tau>$ = **infinite cyclic group** of integer translations.



Vertical Mirror Reflections

$v: (x,y) \rightarrow (-x,y)$, $v^2=1$

For example we might have a reflection symmetry w.r.t the x-axis and/or the y-axis. Such a symmetry of the basic pattern will yield immediately corresponding symmetries of the frieze.

Let us denote by v the vertical symmetry

$$v : (x, y) \longmapsto (-x, y)$$

and by

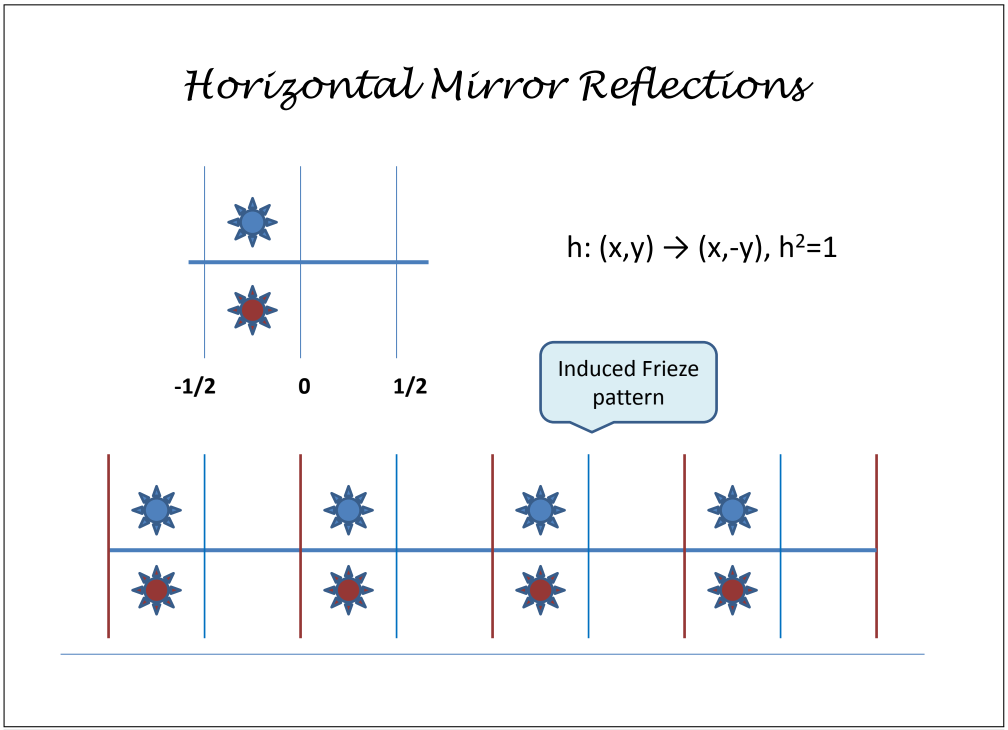
$$h : (x, y) \longmapsto (x, -y),$$

the horizontal symmetry.

Clearly we have $v^2 = e,\ h^2 = e$, since these are both reflection isometries. We have

$$hv = vh : (x, y) \longmapsto (-x, -y),$$

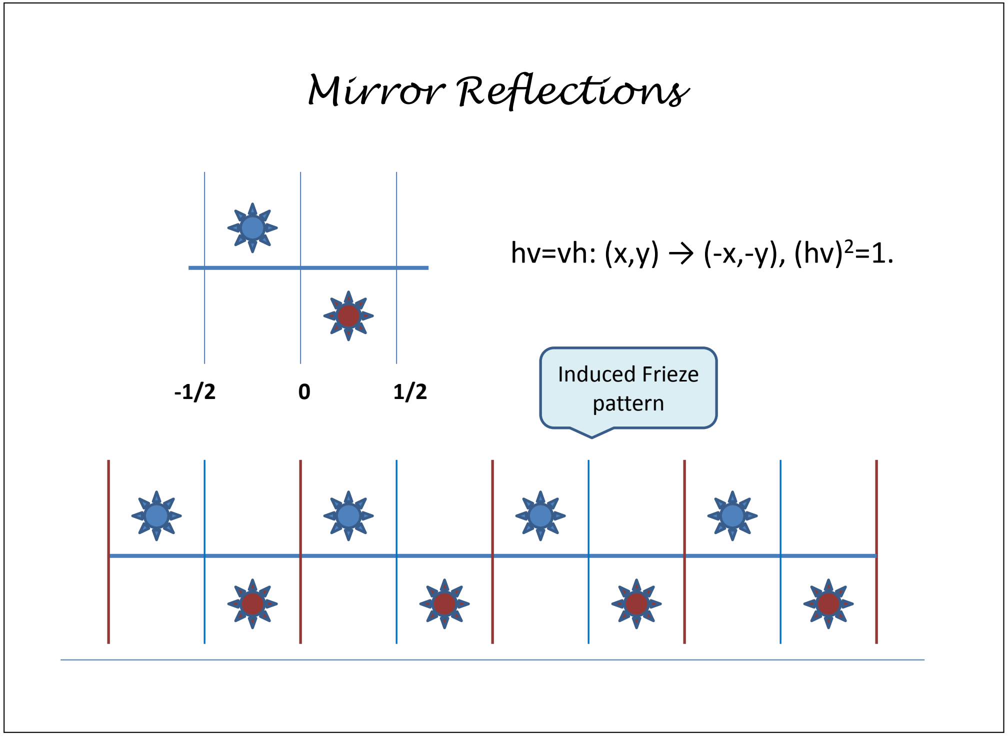
a rotation by 180 degrees, yet another possible symmetry that the basic shape can have.



Horizontal Mirror Reflections

$h: (x,y) \to (x,-y)$, $h^2=1$

Induced Frieze pattern



Mirror Reflections

$hv=vh: (x,y) \to (-x,-y)$, $(hv)^2=1$.

Induced Frieze pattern

Notice that all the frieze symmetries will leave the x-axis invariant (i.e., will map it to itself). The subgroup of isometries that map the x-axis to itself contains all isometries that combine:

1. translations along the x-direction
2. reflections about the x-axis
3. reflection about any axis perpendicular to x
4. glide reflections along the x-direction
5. rotations by $180°$ or its multiples centered on the x-axis.

The study of frieze groups is in fact the study of all subgroups of this group that are discrete, hence their subgroup of translations will have to be $\langle\tau\rangle$ where the unit of translation is the minimal one reproducing the frieze!

To complete the possible symmetries that friezes can have, we must also consider glide reflections that preserve the x-axis. Denote by γ a glide reflection about x, i.e.,

$$\gamma : (x, y) \longmapsto (x + a, -y).$$

We clearly have

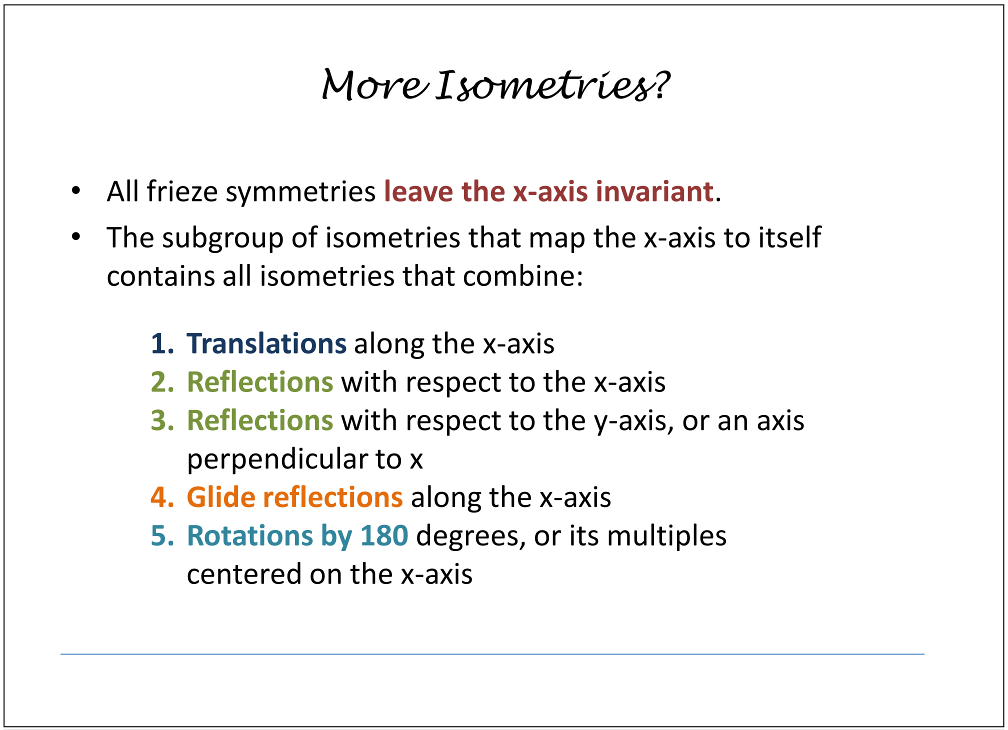
$$\gamma^2 : (x, y) \longmapsto (x + 2a, y),$$

i.e., a translation by twice a as defined above. Therefore taking $a = 1/2$ we get

$$\begin{aligned} \gamma &: (x, y) \longmapsto (x + \frac{1}{2}, -y) \\ \gamma^2 &: (x, y) \longmapsto (x + 1, y), \end{aligned}$$

hence $\gamma^2 = \tau$.

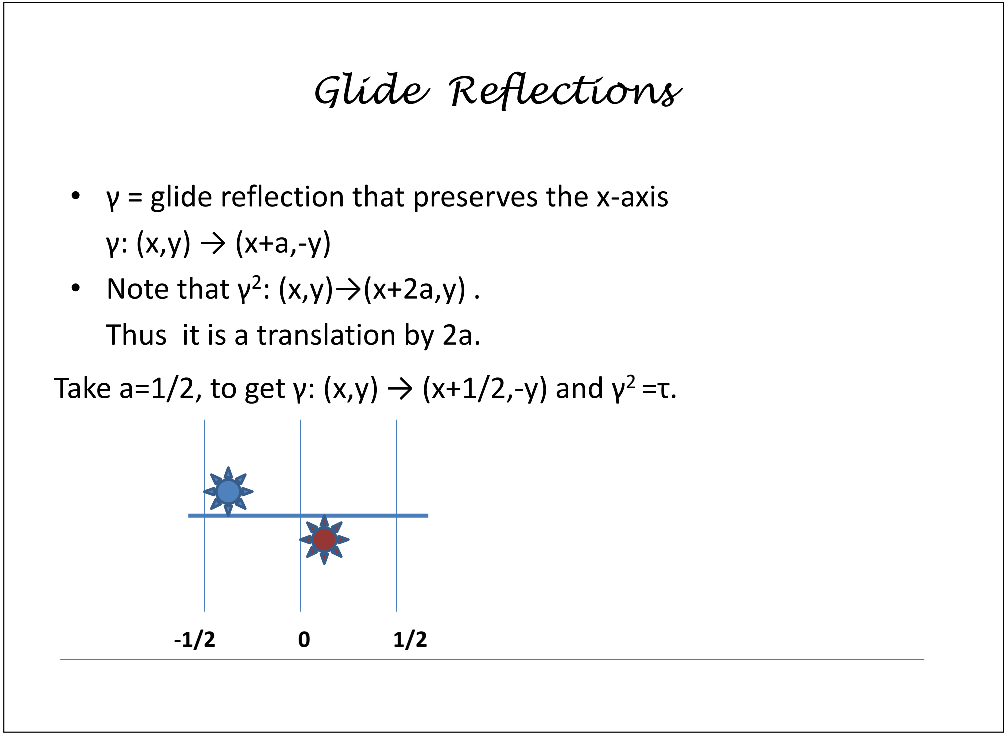
Therefore we can generate τ by applying γ twice.



More Isometries?

- All frieze symmetries **leave the x-axis invariant**.
- The subgroup of isometries that map the x-axis to itself contains all isometries that combine:

1. **Translations** along the x-axis
2. **Reflections** with respect to the x-axis
3. **Reflections** with respect to the y-axis, or an axis perpendicular to x
4. **Glide reflections** along the x-axis
5. **Rotations by 180** degrees, or its multiples centered on the x-axis



Glide Reflections

- γ = glide reflection that preserves the x-axis

  $\gamma: (x,y) \rightarrow (x+a,-y)$
- Note that $\gamma^2: (x,y) \rightarrow (x+2a,y)$.

  Thus it is a translation by 2a.

Take $a=1/2$, to get $\gamma: (x,y) \rightarrow (x+1/2,-y)$ and $\gamma^2 = \tau$.

Theorem 17. *All transformations that preserve the* x*-axis and have as subgroups of translations* $\langle \tau \rangle$ *can be generated by* r, h, γ*, hence all frieze groups must be subgroups of* $\langle v, h, \gamma \rangle$ *.*

Proof.

1. Any translation by integers can be generated. This is true since $\gamma^2 = \tau$, hence we have $\langle \gamma^2 \rangle = \langle \tau \rangle$.
2. Any horizontal reflection can be generated: true because we have h.
3. Any reflection in a frieze will be about an integer or about an half integer point. Let v_p be any vertical reflection. Then

   $$v_p : (x, y) \longmapsto (2p - x, y) \Rightarrow v_p v(x, y) = v_p(-x, y) = (x + 2p, y),$$

   hence $2p$ is an integer because we only allow integer translations and v_p is generated by ($v_p v$ is a translation, thus some power of $\tau = \gamma^2$):

   $$v_p v = (\gamma^2)^k \Rightarrow v_p = (\gamma^2)^k v.$$

4. Consider a half turn about a point P

   $$T_P : (x, y) \mapsto (2p - x, -y).$$

   Then $T_P h = v_p$ and we must have $T_P = v_p h = (\gamma^2)^k r h$.

5. Any glide reflection can be written as

   $$G_p : (x, y) \mapsto (x + p, -y),$$

   hence p is an integer and $G_p h = (\gamma^2)^k \Rightarrow G_p = (\gamma_2)^k h$. Hence all glide reflections possible are generated.

$\square$

After showing that $\langle r, h, \gamma \rangle$ included all possible frieze groups, we must show that there are some restrictions too, hence we cannot have all $\langle r, h, \gamma \rangle$-subgroups as frieze groups.

Theorem 18. h *and* γ *cannot occur together in a frieze group.*

Proof. $hr : (x, y) \mapsto (x + \frac{1}{2}, y)$. But we cannot have translation of $\frac{1}{2}$ in the frieze group since then the frieze would have a periodicity of $\frac{1}{2}$ (and we assume that the least periodicity is 1). $\square$

These results yield all possible frieze groups as the subgroups of $\langle r, h, \gamma \rangle$.

First Theorem

All transformations that preserve the x-axis and have as subgroup <τ> can be generated by v,h,γ, hence all frieze groups must be a subgroup of <v,h,γ>.

Recall the transformations that preserve the x-axis

1. **Translations** along the x-axis
2. **Reflections** with respect to the x-axis
3. **Reflections** with respect to the y-axis, or an axis perpendicular to x
4. **Glide reflections** along the x-axis
5. **Rotations by 180** degrees, or its multiples centered on the x-axis

Second Theorem

h and γ cannot occur together in a frieze group.

Proof. If h and γ belong to the group, then so does hγ.
But then hγ (x,y)=h (x+1/2,-y) = (x+1/2,y).

Contradicts the periodicity of 1 of the frieze pattern.

This theorem gives a classification of Frieze groups.

Theorem 19. *The frieze groups that have no glide reflection symmetries are*

$$\left\langle\gamma^2\right\rangle,\ \left\langle h,\gamma^2\right\rangle,\ \left\langle r,\gamma^2\right\rangle,\ \left\langle hr,\gamma^2\right\rangle,\ \left\langle r,h,\gamma^2\right\rangle.$$

The frieze groups that contain glide reflections are

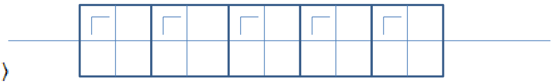
$$\langle\gamma\rangle,\ \langle r,\gamma\rangle.$$

Proof. The first group contains γ^2 with all possible combinations of h, r, γ^2. The second group of friezes contains glide reflections but γ cannot occur with h. It can occur with hr however, because we have

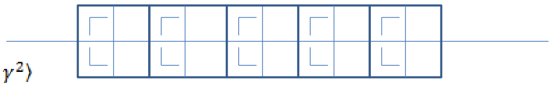
$$\begin{aligned} hr &: (x,y)\mapsto(-x,-y) \\ hr\gamma &: (x,y)\mapsto(-x-\frac{1}{2},y) \end{aligned}$$

It follows that this is the same as (r,γ) with shifted symmetry axes. $\square$

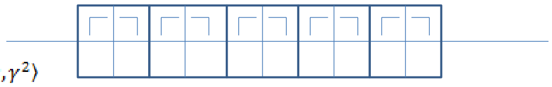
A nice pictorial representation of friezes that have the above 7 types of symmetries is given below.



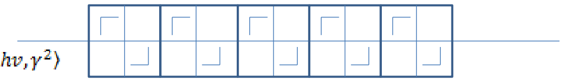
$\langle\gamma^2\rangle$



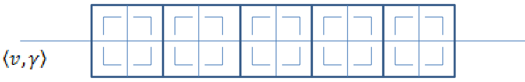
$\langle h,\gamma^2\rangle$



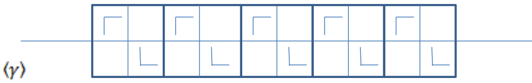
$\langle v,\gamma^2\rangle$



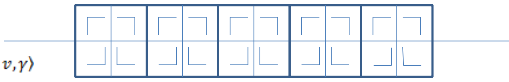
$\langle hv,\gamma^2\rangle$



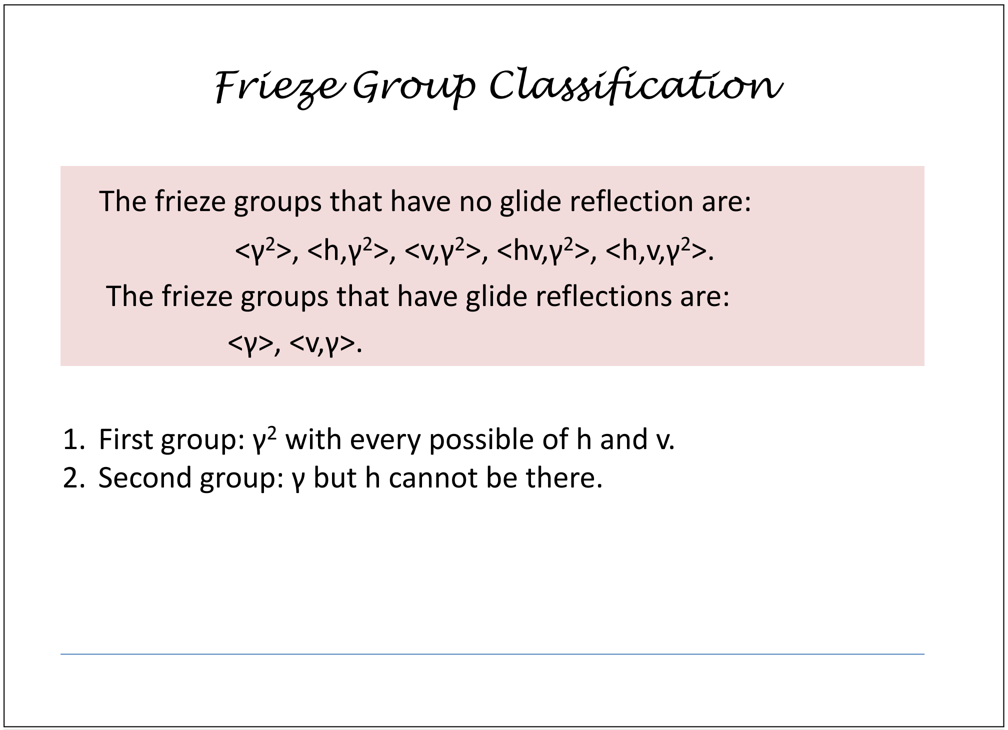
$\langle v,\gamma\rangle$



$\langle\gamma\rangle$



$\langle h,v,\gamma\rangle$



Frieze Group Classification

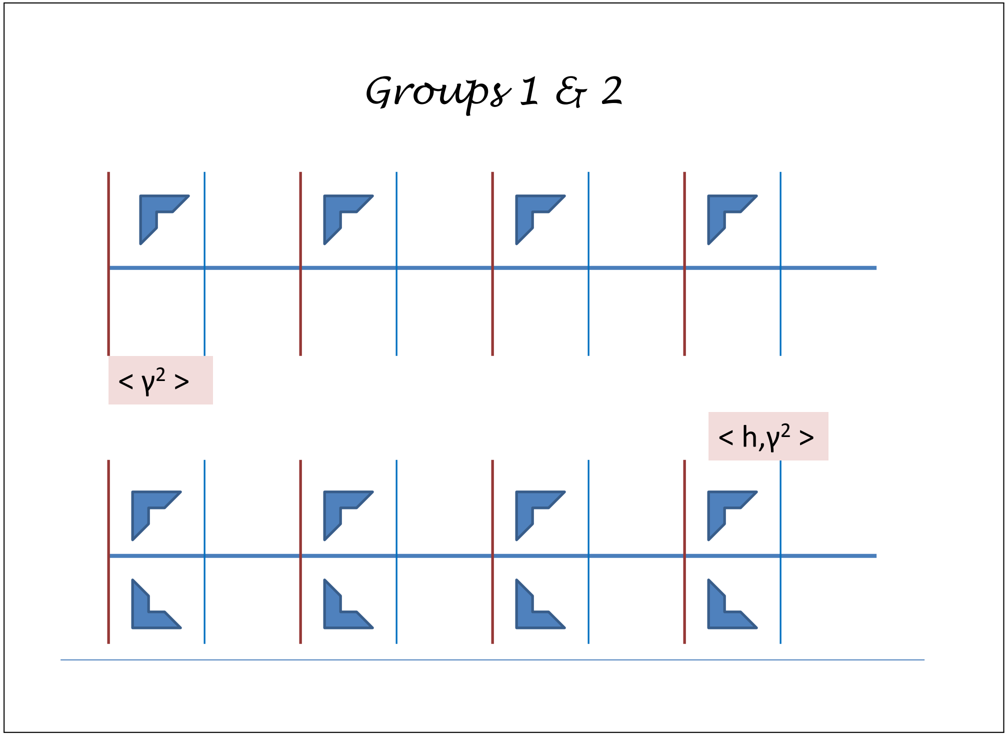
The frieze groups that have no glide reflection are:

$\langle\gamma^2\rangle, \langle h,\gamma^2\rangle, \langle v,\gamma^2\rangle, \langle hv,\gamma^2\rangle, \langle h,v,\gamma^2\rangle$.

The frieze groups that have glide reflections are:

$\langle\gamma\rangle, \langle v,\gamma\rangle$.

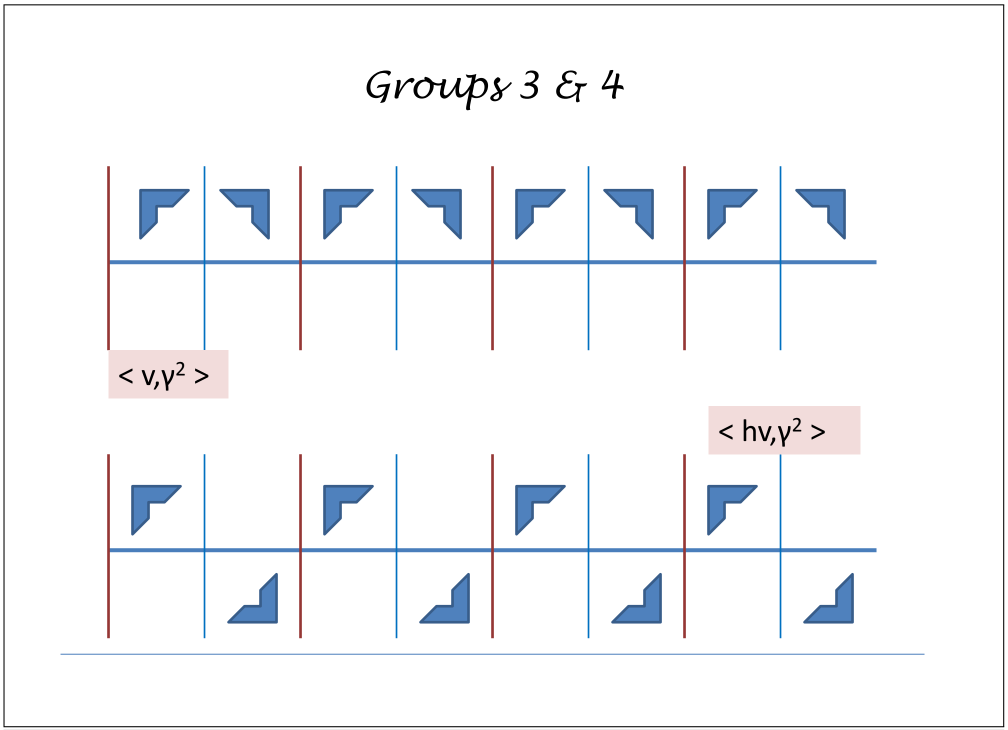
1. First group: γ^2 with every possible of h and v.
2. Second group: γ but h cannot be there.



Groups 1 & 2

$< \gamma^2 >$

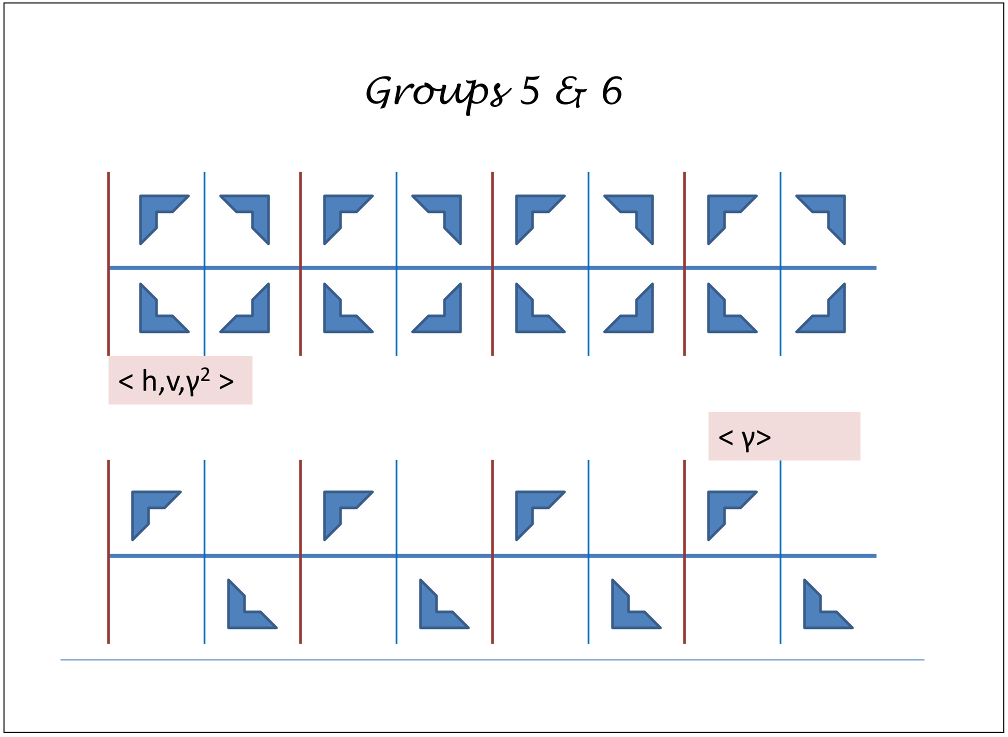
$< h,\gamma^2 >$



Groups 3 & 4

$< v,\gamma^2 >$

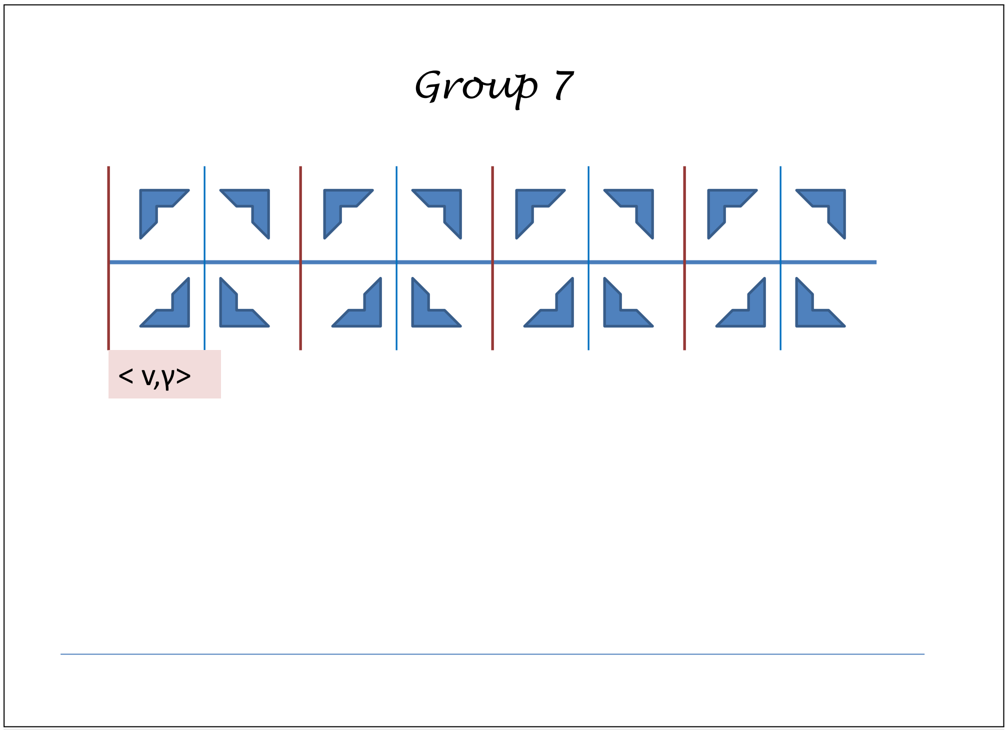
$< hv,\gamma^2 >$



Groups 5 & 6

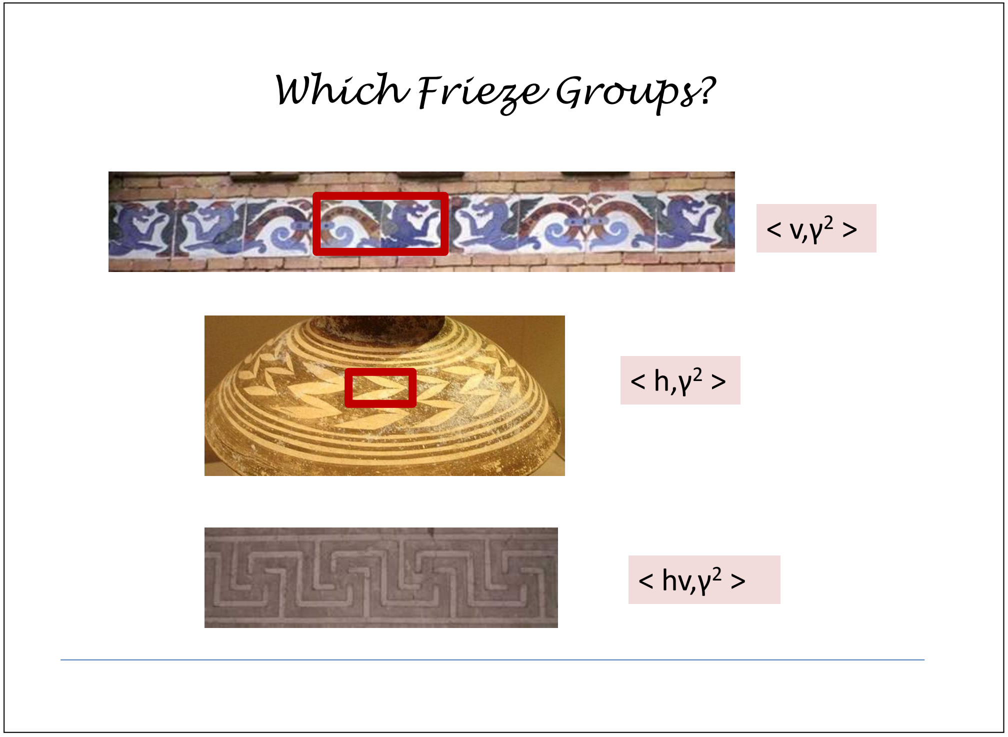
$< h,v,\gamma^2 >$

$< \gamma>$



Group 7

$< v,\gamma>$



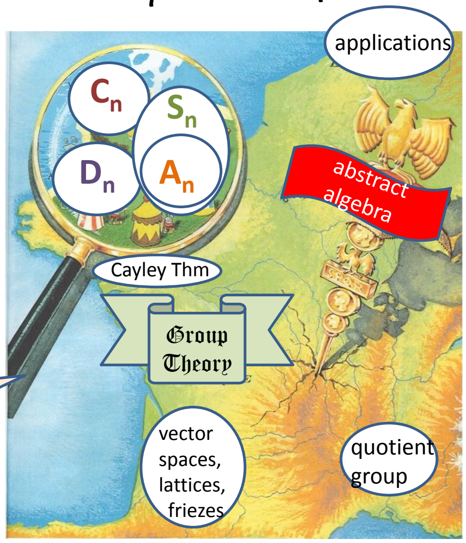
Which Frieze Groups?

$< v,\gamma^2 >$

$< h,\gamma^2 >$

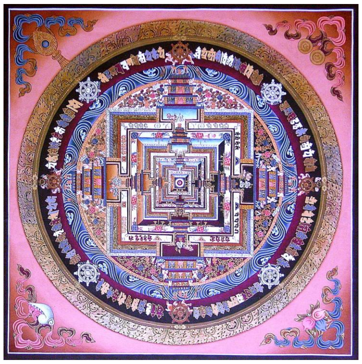
$< hv,\gamma^2 >$

Road Map: End of the Trip!



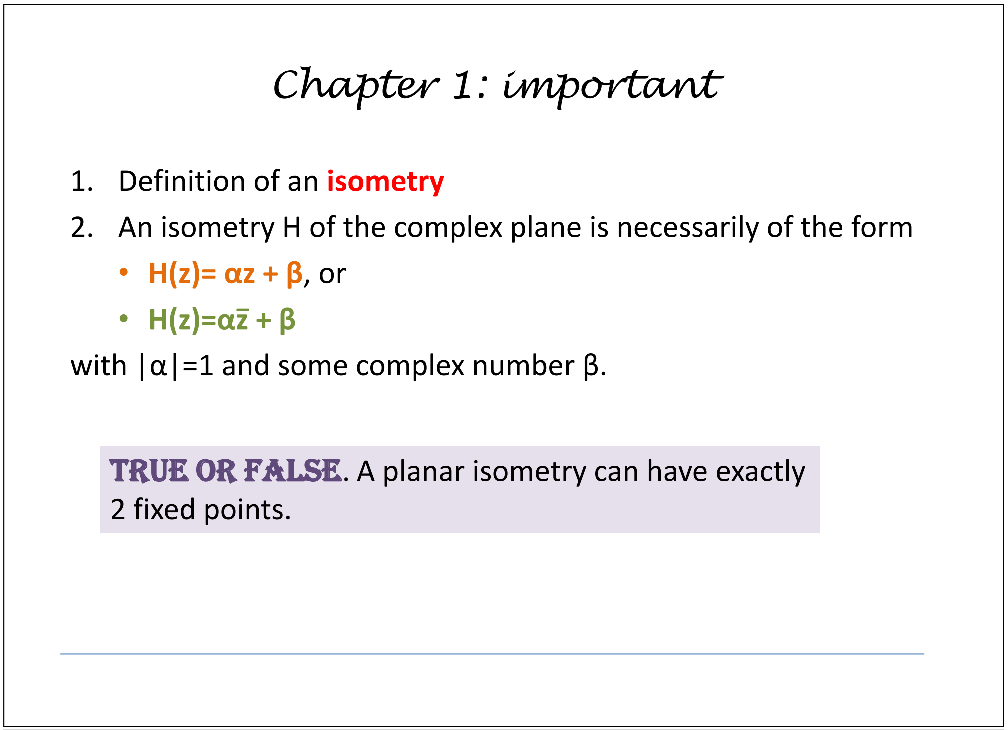
Zoom inside finite group theory!

Chapter 1: Isometries of the Plane



1. Planar isometries (rotation, translation, reflections, glide translations)
2. Classification of the isometries of the plane

Mandalas have a rich group of isometries!

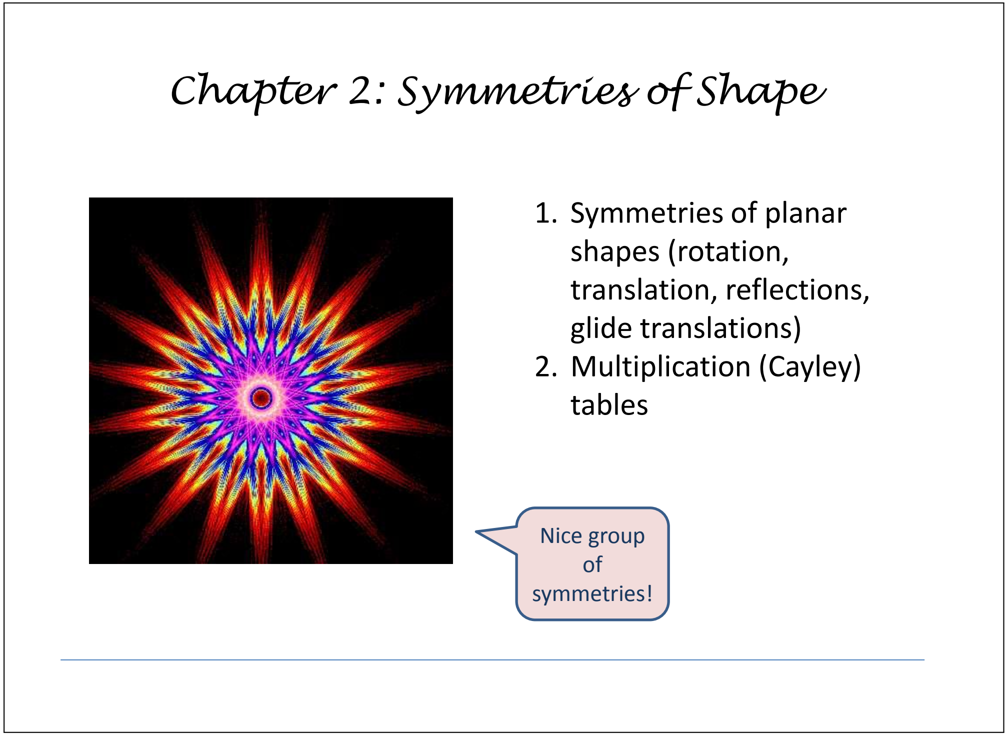


Chapter 1: important

1. Definition of an **isometry**
2. An isometry H of the complex plane is necessarily of the form
   - **H(z)= αz + β**, or
   - **H(z)=α$\bar{z}$ + β**

with |α|=1 and some complex number β.

TRUE OR FALSE. A planar isometry can have exactly 2 fixed points.



Chapter 2: Symmetries of Shape

1. Symmetries of planar shapes (rotation, translation, reflections, glide translations)
2. Multiplication (Cayley) tables

Nice group of symmetries!

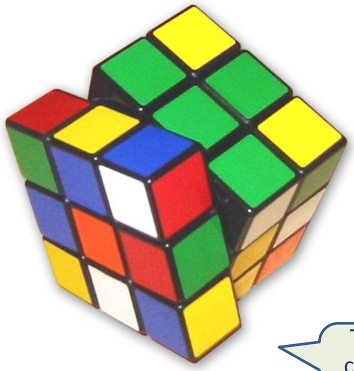
Chapter 2: important

1. Definition of a **symmetry**
2. How to compute **multiplication (Cayley) tables**.

   They illustrate:
   - Closure (every row contains all the symmetries)
   - Inverse (every row contains the identity map)
   - Whether commutativity holds

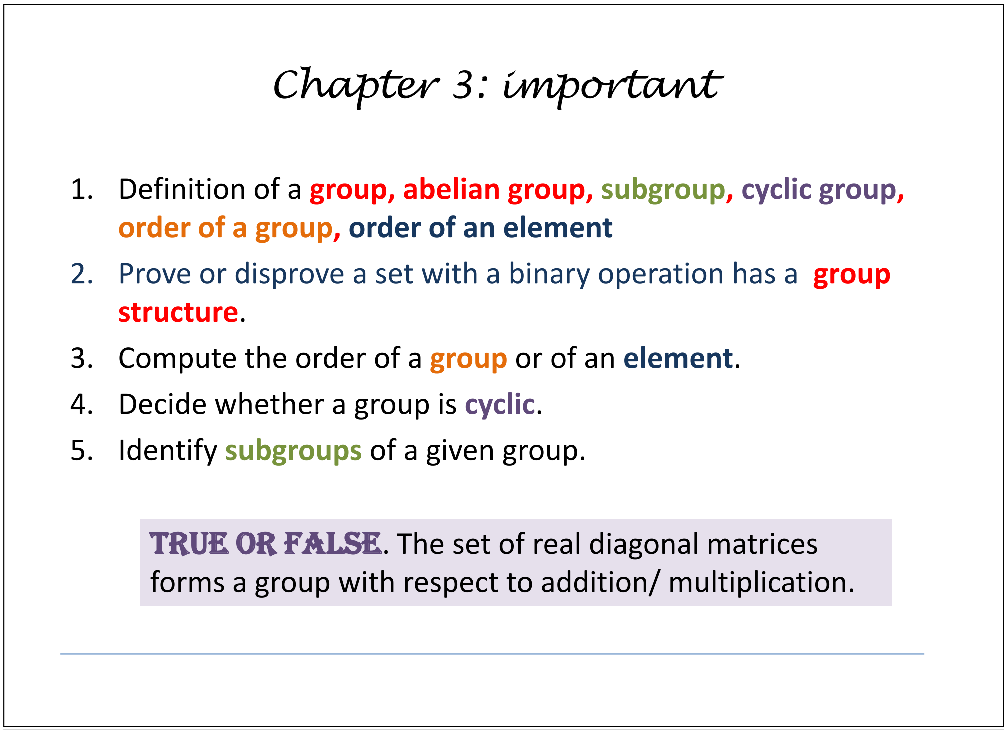
TRUE OR FALSE. Combining two symmetries of the same shape gives another symmetry of this shape.

Chapter 3: Introducing Groups



The rubik cube has a group structure!

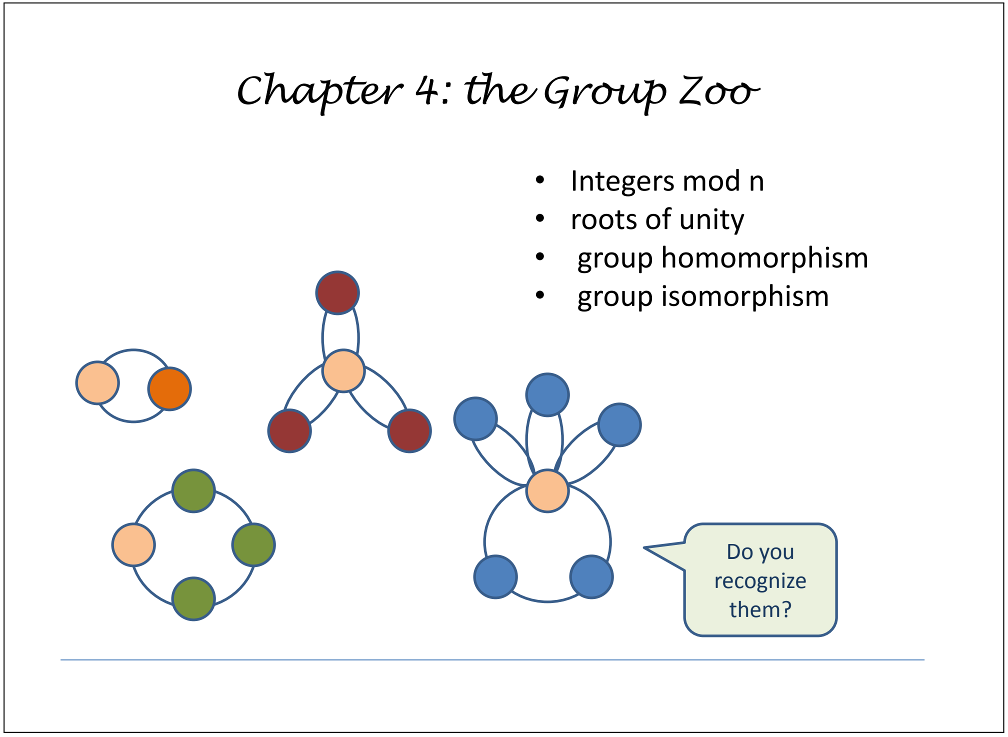
Definition of
- group
- abelian group
- order of group
- order of element
- cyclic group
- subgroup



Chapter 3: important

1. Definition of a **group, abelian group, subgroup, cyclic group, order of a group, order of an element**
2. Prove or disprove a set with a binary operation has a **group structure**.
3. Compute the order of a **group** or of an **element**.
4. Decide whether a group is **cyclic**.
5. Identify **subgroups** of a given group.

TRUE OR FALSE. The set of real diagonal matrices forms a group with respect to addition/ multiplication.



Chapter 4: the Group Zoo

- Integers mod n
- roots of unity
- group homomorphism
- group isomorphism

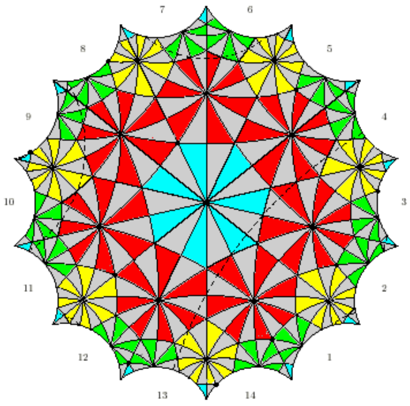
Do you recognize them?

Chapter 4: important

1. Understand **integers mod n**
2. The notion of **group homomorphism**.
3. The notion of **group isomorphism** and how to show that two groups are **isomorphic**.

TRUE OR FALSE. The Klein group is isomorphic to the cyclic group of order 4.

Chapter 5: more Group Structure

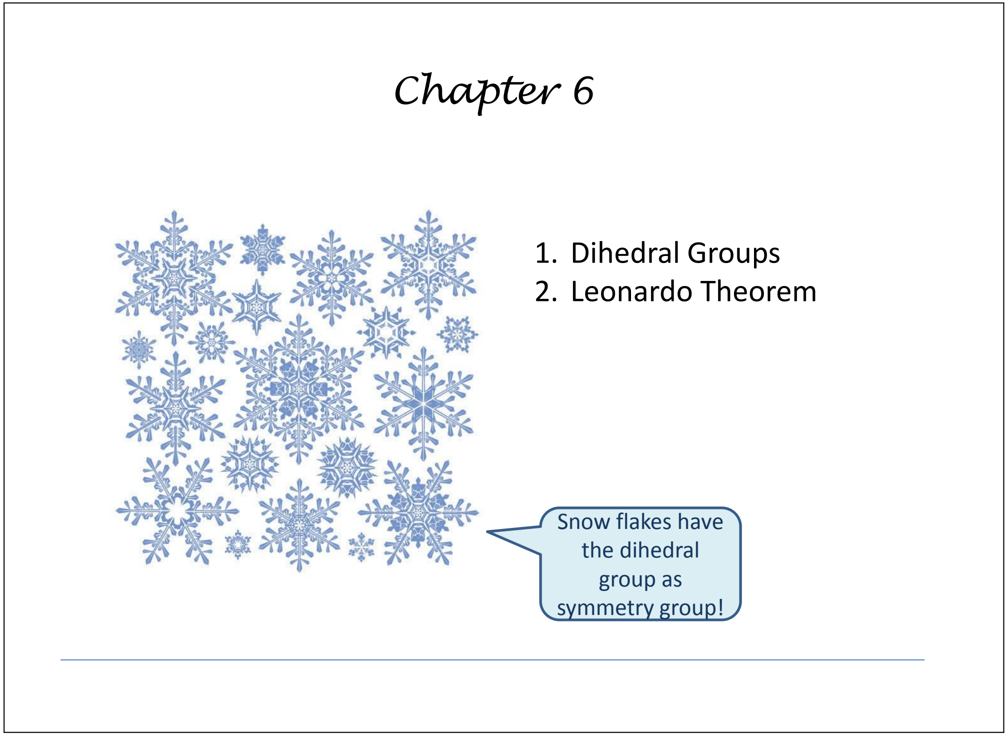


1. Cyclic groups
2. Cosets, Lagrange Theorem and its corollaries.

Chapter 5: important

1. **Cyclic group of order n**
2. **Lagrange theorem and its corollaries**.
3. The notion of **group isomorphism** and how to show that two groups are **isomorphic**.

TRUE OR FALSE. The Dihedral group D_{25} contains an element of order 11.



Chapter 6

1. Dihedral Groups
2. Leonardo Theorem

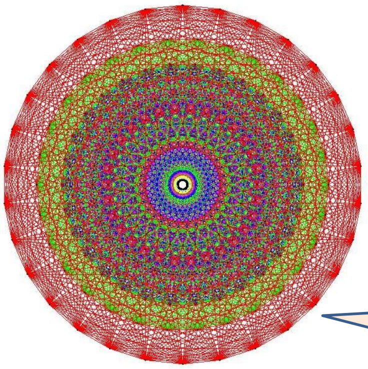
Snow flakes have the dihedral group as symmetry group!

Chapter 6: important

1. **What is a dihedral group**
2. **The statement of Leonardo Theorem**.

TRUE OR FALSE. The symmetric group S_4 of all permutations on 4 elements can be interpreted as a group of planar symmetries.

Chapter 7: Permutation Groups



- Permutations
- parity of a permutation
- symmetric and alternating group

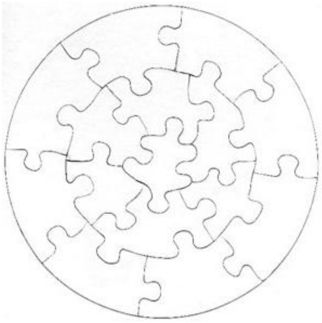
This is the permutation group of some complicated object (related to Lie algebras)!

Chapter 7: important

1. **Formal definition of a permutation**
2. **Parity of a permutation**.

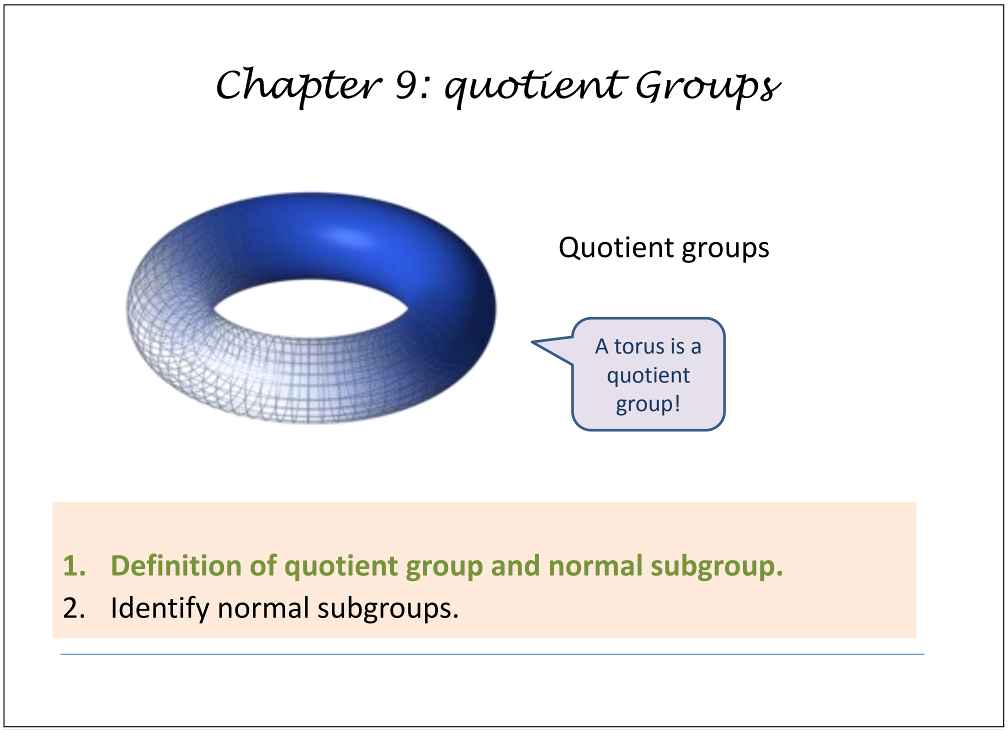
TRUE OR FALSE. A permutation can have two different parities.

Chapter 8: Cayley Theorem, puzzles



- Cayley Theorem
- Puzzles (15 puzzle, solitaire game)
- Cryptography applications (Caesar's cipher, check digit)

1. **Cayley Theorem**
2. Interpret a group as a subgroup of the symmetric group.

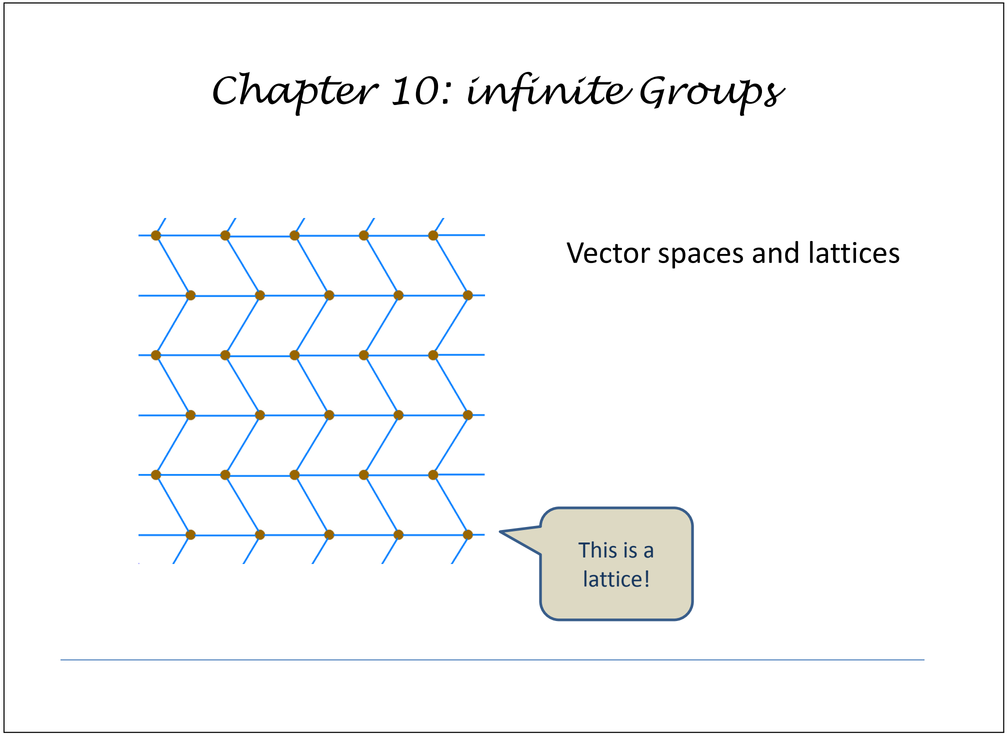


Chapter 9: quotient Groups

Quotient groups

A torus is a quotient group!

1. **Definition of quotient group and normal subgroup.**
2. Identify normal subgroups.



Chapter 10: infinite Groups

Vector spaces and lattices

This is a lattice!

Chapter 12

Revision Exercises

Here are a few extra exercises that serve as revision.

Exercise 48. Lagrange Theorem is likely to be the most important theorem of group theory, so let us revise it! Here is a bit of theory first:

- Can you remember what it states?
- The proof of Lagrange Theorem relies on a counting argument, based on the fact that cosets partition the group. Can you remember what cosets partition the group mean? If so, can you rederive the counting argument that proves Lagrange Theorem?

Now some more practice on how to use Lagrange Theorem!

- How many groups of order 5 do we have (up to isomorphism)?
- Consider the group of permutations S_5. Does S_5 contain a permutation of order 7?
- Suppose there exists an abelian group G of order 12 which contains a subgroup H of order 4. Show that the set of cosets of H forms a group. What is the order of G/H? Deduce what group G/H is.

Exercise 49. At the beginning of the class, we started by studying structure of geometric figures. We have seen shapes, and been asked what is their group of symmetries.

- Can you remember some of the shapes we studied, and what is the corresponding group of symmetries?

- Do you remember what are all the possible groups arising as symmetries of planar shapes?
- Let us do the reverse exercise: think of a symmetry group, and try to draw a figure that has this symmetry group.

Exercise 50. Let us remind a few things about permutations.

- What is the formal definition of a permutation?
- What is the parity of a permutation?
- Consider the permutation σ that maps:

  $$1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 5, 4 \mapsto 3, 5 \mapsto 6, 6 \mapsto 4, 7 \mapsto 7.$$

  Compute its parity.
- We have studied that the group of symmetries of a planar shape can be seen as a group of permutations. Do you remember how that works (either in general or on an example?)

Exercise 51. Let us remember that planar isometries are either of type I: $H(z) = \alpha z + \beta,\ |\alpha| = 1$ or of type II: $H(z) = \alpha \bar{z} + \beta,\ |\alpha| = 1$.

- Show that the isometries of type I form a subgroup H of the group G of planar isometries.
- Show that G/H is a quotient group of order two.

Chapter 13

Solutions to the Exercises

> *"Intuition comes from experience, experience from failure, and failure from trying."*

Exercises for Chapter 1

Exercise 1. Let X be a metric space equipped with a distance d. Show that an isometry of X (with respect to the distance d) is always an injective map.

This exercise shows that one can study isometries in a much more general setting than just in the real plane! In that case, we can only deduce injectivity from the fact that the distances are preserved. It is also useful to recall the definition of a metrice space. Consider a set X and define on pairs of elements of X a map called a distance $d : X \times X \to \mathbb{R}$ *with the properties that*

1. $d(x, y) \geq 0$ *for all* $x, y \in X$*, and* $d(x, y) = 0 \iff x = y$ *(a distance is positive).*
2. $d(x, y) = d(y, x)$ *for all* $x, y \in X$ *(a distance is symmetric).*
3. $d(x, y) + d(y, z) \geq d(x, z)$ *for all* $x, y, z \in X$ *(triangle inequality).*

Solution. Let φ be an isometry of X. We have to show that if $\varphi(x) = \varphi(y)$ for $x, y \in X$, then $x = y$. Now by definition of isometry

$$d(\varphi(x), \varphi(y)) = d(x, y)$$

so if $\varphi(x) = \varphi(y)$, then

$$0 = d(\varphi(x), \varphi(y)) = d(x, y)$$

and $x = y$. Note that $d(x, y) = 0$ implies that $x = y$ is part of the axioms of a distance!

Exercise 2. Recall the general formula that describes isometries H of the complex plane. If a planar isometry H has only one fixed point which is $1+i$, and H sends $1-i$ to $3+i$, then $H(z) =$ __________.

Guided version.

1. Recall the general formula that describes isometries H of the complex plane. We saw that an isometry of the complex plane can take two forms, either $H(z) = \ldots$, or $H(z) = \ldots$
2. You should have managed to find the two formulas, because they are in the lecture notes! Now you need to use the assumptions given. First of all, we know that H has only one fixed point, which is $1+i$. Write in formulas what it means that $1+i$ is a fixed point of H (write it for both formulas).
3. Now you must have got one equation from the previous step. Use the next assumption, namely write in formulas what it means that H sends $1-i$ to $3+i$, this should give you a second equation.
4. If all went fine so far, you must be having two equations, with two unknowns, so you are left to solve this system!
5. Once the system is solved, do not forget to check with the original question to make sure your answer is right!

We will provide two solutions for this question. Here is the first one, which is done from scratch.

Solution. We remember that the general formula for a planar isometry is either $H(z) = \alpha z + \beta$, or $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$. In the first case, that is $H(z) = \alpha z + \beta$, $|\alpha| = 1$, we compute

$$\begin{cases} 1+i &= H(1+i) &= \alpha(1+i)+\beta \\ 3+i &= H(1-i) &= \alpha(1-i)+\beta \end{cases} \Longrightarrow -2 = 2\alpha i \Longrightarrow \begin{cases} \alpha &= i \\ \beta &= 2 \end{cases}$$

We find that $H(z) = \underline{iz+2}$. Now the question states that there is only one fixed point. Let us check that this is true:

$$H(z) = iz + 2 = z \iff z(i-1) = -2 \iff z = \frac{2}{1-i} = 1+i.$$

Since we have only one fixed point, the one we wanted, the answer is $H(z) = \underline{iz+2}$. Now in the second case that is $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$, we again compute

$$\begin{cases} 1+i & = H(1+i) & = \alpha(1-i) + \beta \\ 3+i & = H(1-i) & = \alpha(1+i) + \beta \end{cases} \Longrightarrow -2 = -2\alpha i \Longrightarrow \begin{cases} \alpha & = -i \\ \beta & = 2i+2 \end{cases}$$

We find that $H(z) = -i\bar{z} + 2i + 2$. Now the question states that there is only one fixed point. Let us check that this is true:

$$H(z) = -i\bar{z}+2i+2 = z \iff z_0+iz_1 = -i(z_0-iz_1)+2i+2 \iff z_0+z_1 = 2.$$

We see that $z = 1+i$ is indeed a fixed point, however, it is not the only one! This shows that the final answer to this question is

$$H(z) = \underline{iz+2}.$$

Here is the second solution, which uses Exercise 3!

Solution. If you remember Exercise 3, then you can alternatively solve the exercise this way. In Exercise 3, we investigated the fixed points of a planar isometry, and found the following:

- $H(z) = \alpha z + \beta$, $|\alpha| = 1$:
  - All points are fixed when $\alpha = 1$ and $\beta = 0$;
  - No fixed point when $\alpha = 1$ and $\beta \neq 0$;
  - One and only one fixed point $\frac{\beta}{1-\alpha}$ when $\alpha \neq 1$.
- $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$ ($\alpha = e^{i\theta}$ and $\beta = s + it$):
  - No fixed point when $s \cdot \cos\frac{\theta}{2} + t \cdot \sin\frac{\theta}{2} \neq 0$;
  - The line $2\sin^2\frac{\theta}{2} \cdot x - 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} \cdot y = s$ is fixed when $s \cdot \cos\frac{\theta}{2} + t \cdot \sin\frac{\theta}{2} = 0$.

In fact, you do not need to remember all of that, it is enough that you remember that in the second case, if $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$, there is never a unique fixed point: either we have no fixed point, or we have a line. Since there is one and only one fixed point, we only need to look at the case $H(z) = \alpha z + \beta$, $|\alpha| = 1$. Then

$$\left\{ \begin{array}{lll} 1+i & = H(1+i) & = \alpha(1+i)+\beta \\ 3+i & = H(1-i) & = \alpha(1-i)+\beta \end{array} \right. \Longrightarrow -2 = 2\alpha i \Longrightarrow \left\{ \begin{array}{ll} \alpha & = i \\ \beta & = 2 \end{array} \right.$$

So the answer is $H(z) = \underline{iz+2}$.

Exercise 3. Recall the general formula that describes isometries H of the complex plane. If a planar isometry H fixes the line $y = x+1$ (identifying the complex plane with the 2-dimensional real plane), then $H(z) =$ ________.

We can solve this exercise in two different ways, as we did for the previous exercise. Let us start from scratch.

Solution. Suppose that $H(z) = \alpha z + \beta$, $|\alpha| = 1$ first. If H fixes the line $y = x+1$, this means that H fixes all the points on this line, so we can take two convenient points:

$$y = 0,\ x = -1,\ \text{and}\ x = 0,\ y = 1$$

which in the complex plane correspond to $z = x+iy = -1$ and $z = x+iy = i$ respectively. Now

$$\left\{ \begin{array}{lll} i & = H(i) & = \alpha i+\beta \\ -1 & = H(-1) & = -\alpha+\beta \end{array} \right. \Longrightarrow -1+i = \alpha(i-1) \Longrightarrow \left\{ \begin{array}{ll} \alpha & = 1 \\ \beta & = 0 \end{array} \right.$$

This gives us the identity map! We now consider $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$, and the same two convenient points on the line $y = x+1$: $z = i$ and $z = -1$. We solve

$$\left\{ \begin{array}{lll} i & = H(i) & = \alpha(-i)+\beta \\ -1 & = H(-1) & = \alpha(-1)+\beta \end{array} \right. \Longrightarrow i+1 = (1-i)\alpha \Longrightarrow \left\{ \begin{array}{ll} \alpha & = i \\ \beta & = i-1 \end{array} \right.$$

So the answer is $H(z) = \underline{iz-1+i}$. We can check that the fixed points are indeed the line mentioned.

Now if we remember Exercise 3, we can do as follows (the same thing as in the previous exercise).

Solution. Recall again Exercise 3, where we investigated the fixed points of a planar isometry:

- $H(z) = \alpha z + \beta$, $|\alpha| = 1$:
    - All points are fixed when $\alpha = 1$ and $\beta = 0$;
    - No fixed point when $\alpha = 1$ and $\beta \neq 0$;
    - One and only one fixed point $\frac{\beta}{1-\alpha}$ when $\alpha \neq 1$.
- $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$ ($\alpha = e^{i\theta}$ and $\beta = s + it$):
    - No fixed point when $s \cdot \cos\frac{\theta}{2} + t \cdot \sin\frac{\theta}{2} \neq 0$;
    - The line $2\sin^2\frac{\theta}{2} \cdot x - 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} \cdot y = s$ is fixed when $s \cdot \cos\frac{\theta}{2} + t \cdot \sin\frac{\theta}{2} = 0$.

Since the fixed points form a line, we know that it cannot be $H(z) = \alpha z + \beta$, because then it never happens that only a line is fixed. Thus we only need to consider $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$. Take the same two convenient points on the line $y = x + 1$: $z = i$ and $z = -1$ and solve

$$\begin{cases} i & = H(i) & = \alpha(-i) + \beta \\ -1 & = H(-1) & = \alpha(-1) + \beta \end{cases} \Longrightarrow i + 1 = (1 - i)\alpha \Longrightarrow \begin{cases} \alpha & = i \\ \beta & = i - 1 \end{cases}$$

So the answer is $H(z) = \underline{iz - 1 + i}$.

Exercise 4. Show that an isometry of the complex plane that fixes three non-collinear points must be the identity map.

This is a generalization of the Lemma 1 seen in Chapter 1, where we proved almost the same thing. The statement was for three special points, 0, 1 and i. This exercise shows that the points can be anything as long as they are not colinear! You can try to redo the proof step-by-step and see what happens...this is the first solution, or try to use what you now know about planar isometries, this is the second solution below.

Solution. Let H be an isometry of the complex plane which fixes say z_1, z_2, z_3:

$$H(z_1) = z_1,\ H(z_2) = z_2,\ H(z_3) = z_3.$$

We have, by definition of an isometry, that

$$|H(z) - H(z_1)|^2 = |z - z_1|^2$$

thus by developing both the left and the right handside, we get

$$H(z)\overline{H(z)} - H(z)\overline{H(z_1)} - H(z_1)\overline{H(z)} + H(z_1)\overline{H(z_1)} = z\bar{z} - z\bar{z}_1 - z_1\bar{z} + z_1\bar{z}_1.$$

Since we know that $H(z_1) = z_1$, we further simplify to get

$$H(z)\overline{H(z)} - H(z)\bar{z}_1 - z_1\overline{H(z)} + z_1\bar{z}_1 = z\bar{z} - z\bar{z}_1 - z_1\bar{z} + z_1\bar{z}_1,$$

that is

$$H(z)\overline{H(z)} - H(z)\bar{z}_1 - z_1\overline{H(z)} = z\bar{z} - z\bar{z}_1 - z_1\bar{z}.$$

Now we can do the exact same thing by replacing z_1 by z_2, which yields

$$H(z)\overline{H(z)} - H(z)\bar{z}_2 - z_2\overline{H(z)} = z\bar{z} - zz_2 - z_2\bar{z}.$$

So far, everything is pretty much the same as what we did in the class!

Now we notice that $H(z)\overline{H(z)}$ appear on both the left hand sides of the 2 above equations, and $z\bar{z}$ similarly appear on both the right hand sides. Thus we get

$$\begin{aligned} H(z)\overline{H(z)} - z\bar{z} &= H(z)\bar{z}_1 + z_1\overline{H(z)} - z\bar{z}_1 - z_1\bar{z} \\ &= H(z)\bar{z}_2 + z_2\overline{H(z)} - z\bar{z}_2 - z_2\bar{z}, \end{aligned}$$

from which it follows that

$$H(z)\bar{z}_1 + z_1\overline{H(z)} - z\bar{z}_1 - z_1\bar{z} = H(z)\bar{z}_2 + z_2\overline{H(z)} - z\bar{z}_2 - z_2\bar{z}.$$

By rearranging the terms we get

$$(H(z) - z)(\bar{z}_1 - \bar{z}_2) + (\overline{H(z)} - \bar{z})(z_1 - z_2) = 0.$$

So now, we have used two of the three points we have! So we redo everything we did so far with z_1 and z_3 instead of z_1 and z_2, to get

$$(H(z) - z)(\bar{z}_1 - \bar{z}_3) + (\overline{H(z)} - \bar{z})(z_1 - z_3) = 0.$$

Now we can extract $\overline{H(z)} - \bar{z}$ from the second equation above

$$\overline{H(z)} - \bar{z} = \frac{-(H(z) - z)(\bar{z}_1 - \bar{z}_2)}{z_1 - z_2}$$

(note that $z_1 \neq z_2$ so that makes sense, if $z_1 = z_2$, then z_1, z_2, z_3 are then necessarily collinear!), and insert it in the equation that follows to get:

$$(H(z) - z)(\bar{z}_1 - \bar{z}_3) - \frac{(H(z) - z)(\bar{z}_1 - \bar{z}_2)}{z_1 - z_2}(z_1 - z_3) = 0.$$

We can then factor out $H(z) - z$, namely

$$(H(z) - z)\left((\bar{z}_1 - \bar{z}_3) - \frac{(z_1 - z_3)(\bar{z}_1 - \bar{z}_2)}{z_1 - z_2}\right) = 0.$$

We are now almost there! Recall that we want to prove that H is the identity if the three points z_1, z_2, z_3 are not collinear. If we can now prove that

$$(\bar{z}_1 - \bar{z}_3) - \frac{(z_1 - z_3)(\bar{z}_1 - \bar{z}_2)}{z_1 - z_2} \neq 0$$

then it must be that

$$H(z) - z = 0,$$

which concludes the proof! So let us make sure that

$$(\bar{z}_1 - \bar{z}_3) - \frac{(z_1 - z_3)(\bar{z}_1 - \bar{z}_2)}{z_1 - z_2} \neq 0.$$

If this term were to be 0, then

$$(\bar{z}_1 - \bar{z}_3)(z_1 - z_2) = (z_1 - z_3)(\bar{z}_1 - \bar{z}_2),$$

or equivalently

$$\frac{z_2 - z_1}{z_3 - z_1} = \frac{\bar{z}_2 - \bar{z}_1}{\bar{z}_3 - \bar{z}_1}.$$

But this is not possible, because we have assumed that z_1, z_2, z_3 are not collinear. Can you see this? The above equation says that $(z_2 - z_1)/(z_3 - z_1)$ is a real number, this means that if we write $z_2 - z_1$ and $z_3 - z_1$ in polar coordinates, with respective phase ψ_1 and ψ_2, then the complex part of the ratio is $e^{i(\psi_1 - \psi_2)}$, which has to be zero. Thus $\psi_1 = \psi_2$, showing that $z_2 - z_1$ and $z_3 - z_1$ are two vectors centered at the origin pointing in the same direction. In other words, $z_2 - z_1$, $z_3 - z_1$ and 0 are collinear! This shows that z_2, z_3, z_1 are collinear, a contradiction.

Here is another possible solution to this question. The advantage of the above solution is that it assumes nothing on planar isometries, but the computations are a bit lengthy...the advantage of the solution below is that it is pretty short! however you already need to know what are planar isometries!

Solution.

- If $H(z) = \alpha z + \beta$, $|\alpha| = 1$, then

  $$\begin{cases} z_1 = H(z_1) & = \alpha z_1 + \beta \\ z_2 = H(z_2) & = \alpha z_2 + \beta \end{cases} \Longrightarrow z_1 - z_2 = \alpha(z_1 - z_2).$$

  Then we know that α has to be 1. Since $\alpha = 1$, we get $z_1 = z_1 + \beta$ and $z_2 = z_2 + \beta$, which forces β to be 0. Since $\alpha = 1$ and $\beta = 0$, we have that $H(z) = z$ and we are done!

- If $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$, then

  $$\begin{cases} z_1 = H(z_1) & = \alpha\bar{z}_1 + \beta \\ z_2 = H(z_2) & = \alpha\bar{z}_2 + \beta \end{cases} \Longrightarrow z_1 - z_2 = \alpha(\bar{z}_1 - \bar{z}_2).$$

  We do the same thing for z_1 and z_3:

  $$\begin{cases} z_1 = H(z_1) & = \alpha\bar{z}_1 + \beta \\ z_3 = H(z_3) & = \alpha\bar{z}_3 + \beta \end{cases} \Longrightarrow z_1 - z_3 = \alpha(\bar{z}_1 - \bar{z}_3).$$

  Now we put the two equations that we obtained together:

  $$\begin{cases} z_1 - z_2 = \alpha(\bar{z}_1 - \bar{z}_2) \\ z_1 - z_3 = \alpha(\bar{z}_1 - \bar{z}_3) \end{cases} \Longrightarrow \frac{z_1 - z_2}{z_1 - z_3} = \frac{\bar{z}_1 - \bar{z}_2}{\bar{z}_1 - \bar{z}_3}.$$

  To finish the proof, argue as above that this means that z_1, z_2 and z_3 are colinear. In other words, $H(z) = \alpha\bar{z} + \beta$ cannot fix any arbitrary three points unless if they are colinear. Thus an isometry which fixes three arbitrary non-colinear points is of the form $H(z) = \alpha z + \beta$ and we showed that it is then $H(z) = z$.

Exercise 5. In this exercise, we study the fixed points of planar isometries. Recall that a planar isometry is of the form $H(z) = \alpha z + \beta$, $H(z) = \alpha\bar{z} + \beta$, $|\alpha| = 1$. Determine the fixed points of these transformations in the different cases that arise:

1. if $H(z) = \alpha z + \beta$ and $\alpha = 1$,

2. if $H(z) = \alpha z + \beta$ and $\alpha \neq 1$

3. if $H(z) = \alpha \bar{z} + \beta$ and $\alpha = 1$, further distinguish $\beta = 0$ and $\beta \neq 0$,

4. if $H(z) = \alpha \bar{z} + \beta$ and $\alpha \neq 1$, further distinguish $\beta = 0$ and $\beta \neq 0$.

This exercise shows the importance of fixed points. In fact, it is an intermediate step to prove Theorem 2.

Solution. The formula (from Theorem 1) is that an isometry H of the complex plane is given by

$$H(z) = \alpha z + \beta \text{ or } H(z) = \alpha \bar{z} + \beta,$$

where $|\alpha| = 1$.

We now look at the fixed points of these maps. Let us start with

$$\boxed{H(z) = \alpha z + \beta.}$$

If z is a fixed point, then $H(z) = z$, that is

$$\alpha z + \beta = z \iff z(\alpha - 1) + \beta = 0.$$

The case $\alpha = 1$. If $\alpha = 1$, then $\beta = 0$. What it means is: if $\alpha = 1$, then $H(z) = z + \beta$, that is the isometry is a translation, and in that case, a fixed point occurs only when $\beta = 0$, that is the identity map. **If H is a translation, different than the identity, then it has no fixed point.**

The case $\alpha \neq 1$. If $\alpha \neq 1$, we can divide by $1 - \alpha$, to get

$$z = \beta/(1 - \alpha),$$

that is we have only one fixed point. Note that if $\beta = 0$, H is a pure rotation around the origin, and we understand geometrically that there is only one fixed point at $z = 0$. **If $H(z) = \alpha z + \beta$ with $\alpha \neq 1$, then the isometry has only one fixed point given by $z = \beta/(1 - \alpha)$.**

We now continue with the other case, that is

$$\boxed{H(z) = \alpha \bar{z} + \beta.}$$

We have

$$H(z) = z \iff \alpha\bar{z} + \beta = z.$$

Let us write $z = z_0 + iz_1$. Then we can continue to develop

$$H(z) = z \iff \alpha(z_0 - iz_1) + \beta = z_0 + iz_1 \iff z_0(\alpha - 1) + \beta = z_1 i(1 + \alpha).$$

If you look at this last equation as a function of z_0 and z_1, you can see that we will get either a line, or a point, or an empty set. We need to distinguish cases as above to figure out when the different scenarios occur.

The case $\alpha = 1$. If $\alpha = 1$, then

$$\beta = z_1 2i \Rightarrow z_1 = \beta/2i.$$

Since z_1 is a real number, it must be that β is a totally imaginary number, say $\beta = i\beta'$, β' a real number. If we write $\beta = |\beta|e^{i\varphi}$, then $\varphi = \pi/2$, and

$$z_1 = \frac{\beta}{2i} = \frac{|\beta|e^{3i\pi/2}e^{i\varphi}}{2} = \frac{|\beta|}{2}.$$

This shows that **if $H(z) = \bar{z} + \beta$, then $\beta = i|\beta|$ and the fixed points form a line** given by

$$z_1 = \frac{|\beta|}{2}.$$

The case $\alpha \neq 1$, $\beta = 0$. If $\alpha \neq 1$, $\beta = 0$, then

$$z_0(\alpha - 1) = z_1 i(1 + \alpha) \Rightarrow z_0 = z_1 i\frac{1 + \alpha}{\alpha - 1}.$$

We provide two solutions here. Here is the first one:

For this expression to make sense, it must be that the fraction is a totally imaginary number, say $(1+\alpha)/(1-\alpha) = ia$ for some a a real number. Since $|\alpha| = 1$, we have that $\alpha = \cos\theta + i\sin\theta$, and $(1+\alpha)/(1-\alpha) = ia$ becomes $\cos\theta + 1 = -a\sin\theta$ and $\sin\theta = a\cos\theta - a$ that is $\cos\theta = (a^2 - 1)/(a^2 + 1)$. This isometry has for fixed points a line. **If $H(z) = \alpha\bar{z}$, then its fixed points form a line**.

Here is the second solution.

Alternatively, starting again from

$$z_0(\alpha - 1) = z_1 i(1+\alpha),$$

one can start by rewriting α as $\alpha = \cos\theta + i\sin\theta$, yielding

$$z_0(\cos\theta + i\sin\theta - 1) = z_1 i(1 + \cos\theta + i\sin\theta),$$

and by separating real and imaginary part, we get

$$z_0\cos\theta - z_0 + z_1\sin\theta = 0,\ \ z_0\sin\theta - z_1 - z_1\cos\theta = 0.$$

This is a system of linear equations in z_0, z_1, which can be written

$$\begin{pmatrix} \cos\theta - 1 & \sin\theta \\ \sin\theta & -1-\cos\theta \end{pmatrix}\begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

To know whether this system has a solution, we look at the determinant of the matrix, given by 0! This means the matrix is not invertible. If the matrix were invertible, then the only solution would be $(z_0, z_1) = (0,0)$, but since this is not the case, then that means that the solution is a subspace of dimension 1, that is a line (a solution exists, since $(0,0)$ is always a solution).

The case $\alpha \neq 1$, $\beta \neq 0$. Finally, if $\alpha \neq 1$, $\beta \neq 0$, then

$$z_0 = \frac{z_1 i(1+\alpha) - \beta}{\alpha - 1}.$$

Here we can follow either of the above methods, that is either try to determine when

$$\frac{z_1 i(1+\alpha) - \beta}{\alpha - 1}$$

is a real number, or write the system of linear equations.

Here is the first solution.

With the first method, we have that if

$$\frac{z_1 i(1+\alpha) - \beta}{\alpha - 1} = x, x \in \mathbb{R},$$

then

$$z_1 i + z_1 i\cos\theta - z_1\sin\theta - \beta_1 - i\beta_2 = x\cos\theta + xi\sin\theta - x$$

that is, by separating real and imaginary parts

$$z_1 + z_1\cos\theta - \beta_2 = x\sin\theta, \quad -z_1\sin\theta - \beta_1 = x(\cos\theta - 1).$$

By identifying what x should be equal to in both these equations, we get

$$(z_1 + z_1\cos\theta - \beta_2)(\cos\theta - 1) = \sin\theta(-z_1\sin\theta - \beta_1)$$

which after simplifying yields

$$\beta_2(1-\cos\theta) + \beta_1\sin\theta = 0.$$

Thus if β_1, β_2 satisfy this equation, then the fixed point is a line, if not there is no solution. **If $H(z) = \alpha\bar{z}+\beta$, with $\alpha \neq 1$, $\beta \neq 0$, then either the fixed points form a line, if β_1, β_2 satisfies the above equation, or there is none.**

Here is the second solution.

We have that $z_0(\cos\theta + i\sin\theta - 1) + \beta = z_1 i(1+\cos\theta + i\sin\theta)$, where $\beta = \beta_1 + i\beta_2$. By separating real and imaginary parts, we get

$$z_0\cos\theta - z_0 + \beta_1 = -z_1\sin\theta, \; z_0\sin\theta + \beta_2 = z_1 + z_1\cos\theta$$

which corresponds to the following system of linear equations:

$$\begin{pmatrix} \cos\theta - 1 & \sin\theta \\ \sin\theta & -1-\cos\theta \end{pmatrix}\begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = -\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}.$$

The determinant of the matrix is still the same, namely 0, but this time this not clear that a solution always exists. If it does, then we know it is a line. To know when there is no solution, we can use that a rank 1 matrix can be written as the outer product of two vectors, namely

$$\begin{pmatrix} \cos\theta - 1 & \sin\theta \\ \sin\theta & -1-\cos\theta \end{pmatrix} = -2\begin{pmatrix} \sin(\theta/2) \\ -\cos(\theta/2) \end{pmatrix}(\sin(\theta/2), \; -\cos(\theta/2)).$$

Here we use the trigonometric formulas for double/half-angles:

$$\cos(2\gamma) = 2\cos^2(\gamma) - 1 = 1 - 2\sin^2(\gamma), \; \sin(2\gamma) = 2\sin(\gamma)\cos(\gamma).$$

If (β_1, β_2) can be written as a multiple of

$$\begin{pmatrix} \sin(\theta/2) \\ -\cos(\theta/2) \end{pmatrix},$$

then the solution is a line, otherwise there is no solution. We can see that both conditions are of course the same! Indeed if $\beta_1 = a\sin(\theta/2)$, $\beta_2 = -a\cos(\theta/2)$, then

$$-\cos(\theta/2)(1-\cos\theta) + \sin(\theta/2)\sin\theta = 0,$$

and vice-versa, if $\beta_2(1-\cos\theta)+\beta_1\sin\theta = 0$, then $\beta_2\sin(\theta/2)+\beta_1\cos(\theta/2) = 0$ and solutions are indeed of the right form. Now this tells us that

$$\beta = \beta_1 + i\beta_2 = |\beta|(\sin(\theta/2) - i\cos(\theta/2)) = -i|\beta|e^{i\theta/2} = |\beta|e^{i(\theta-\pi)/2}.$$

We now discuss another way of solving this exercise.

Solution. The case $H(z) = \alpha z + \beta$ was less difficult, so we focus on the second case

$$H(z) = \alpha\bar{z} + \beta$$

with $|\alpha| = 1$, which means that we can write $\alpha = e^{i\theta}$ for θ some real number. We now suppose that H has fixed points, and start with finding what β looks like.

Suppose z is fixed by H, that is $H(z) = z$. Then

$$z = H(z) = H(H(z)).$$

Therefore

$$z = \alpha(\overline{\alpha\bar{z}} + \bar{\beta}) + \beta$$

and as $|\alpha| = \alpha\bar{\alpha} = 1$, this gives us

$$z = z + \alpha\bar{\beta} + \beta$$

that is $\alpha\bar{\beta} = -\beta$. We observe that the case $\beta = 0$ needs to be treated separately, so let us assume that $\beta \neq 0$, so that we can conclude that $\alpha = -\beta/\bar{\beta}$. Recall that $\alpha = e^{i\theta}$, and write similarly $\beta = |\beta|e^{i\varphi}$. Then

$$e^{i\theta} = \frac{-e^{i\varphi}}{e^{-i\varphi}} = -e^{2i\varphi} = e^{i\pi+2i\varphi}$$

and we get

$$\theta = \pi + 2\varphi \Rightarrow \varphi = (\theta-\pi)/2$$

and we conclude that

$$\beta = |\beta|e^{i(\theta-\pi)/2}.$$

We can check that this expression for β is consistent with those we got earlier.

Now let us find the fixed points of $H(z)$. Since β is linearly independent from $e^{i\theta/2}$, when perceived as vectors in $\mathbb{R}^2$ (in fact they are perpendicular), we can write every complex number z as an $\mathbb{R}$- linear combination:

$$z = x\beta + ye^{i\theta/2}$$

where $x, y \in \mathbb{R}$ are real scalars. Now let us solve

$$H(z) = \alpha\bar{z} + \beta = z \iff \alpha(x\bar{\beta} + e^{\bar{i}\theta}y) + \beta = x\beta + e^{i\theta/2}y.$$

Opening up the parentheses and recalling that $\alpha = e^{i\theta}$ we get

$$H(z) = \alpha x\bar{\beta} + e^{i\theta/2}y + \beta = x\beta + e^{i\theta/2}y$$

from which we get

$$x(\alpha\bar{\beta} - \beta) + \beta = 0.$$

We solve

$$x = \beta/(\beta - \alpha\bar{\beta}) = \frac{1}{1 - \alpha\bar{\beta}/\beta}$$

recalling the values of α, β we obtain in the denominator

$$1 - \alpha\bar{\beta}/\beta = 1 - e^{i\theta - 2i\phi} = 1 - e^{i\pi} = 2.$$

Hence $x = 1/2$ and y is free, and we obtain that the fixed line is

$$\{\beta/2 + ye^{i\theta/2} \mid y \in \mathbb{R}\}.$$

Exercises for Chapter 2

Exercise 6. Determine the symmetries of an isosceles triangle, and compute the multiplication table of all its symmetries.

Solution. An isosceles triangle has two sides which are equal. Consider a line that goes through the point where both equal sides touch, and crosses the 3rd side in a perpendicular manner. Denote by m the reflection through this line. An isosceles triangle has only two symmetries, the identity map and m. The multiplication table is thus

	1	m
1	1	m
m	m	1

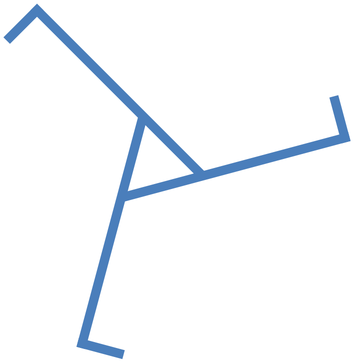
Exercise 7. Determine the symmetries of an equilateral triangle, and compute the multiplication table of all its symmetries.

Solution. Denote by m_1 the reflection that goes through the lower left-hand corner of the triangle, by m_2 the reflection that goes through the lower right-hand corner of the triangle, and by m_3 the vertical reflection. In addition, we have a rotation r of 120 degrees counter clockwise, so that r^2 is the counter clockwise rotation of 240 degrees, and finally 1 denotes the do nothing symmetry.

The multiplication table is found below.

	1	r	r^2	m_3	m_1	m_2
1	1	r	r^2	m_3	m_1	m_2
r	r	r^2	1	m_2	m_3	m_1
r^2	r^2	1	r	m_1	m_2	m_3
m_3	m_3	m_1	m_2	1	r	r^2
m_1	m_1	m_2	m_3	r^2	1	r
m_2	m_2	m_3	m_1	r	r^2	1

Exercise 8. Determine the symmetries of the following shape, and compute the multiplication table of all its symmetries.



Solution. The symmetries of the shape are 1=do-nothing, r=rotation (counterclockwise) of 120 degrees, r^2=rotation (counterclockwise) of 240 degrees. The table is then

	1	r	r^2
1	1	r	r^2
r	r	r^2	1
r^2	r^2	1	r

Exercise 9. Let $z = e^{2i\pi/3}$.

1. Show that $z^3 = 1$.
2. Compute the multiplication table of the set $\{1, z, z^2\}$.
3. Compare your multiplication table with that of Exercise 2. What can you observe? How would you interpret what you can see?

Solution.

1. We have

$$z^3 = (e^{2i\pi/3})^3 = e^{2i\pi} = 1.$$

2. The table is

	1	z	z^2
1	1	z	z^2
z	z	z^2	1
z^2	z^2	1	z

3. We observe that the two tables are the same. The interpretation is that there is a bijection between the rotations of angle 120, 240 and 360 degrees and the powers of z, mapping the rotation r to z.

Exercise 10. In the notes, we computed the multiplication table for the symmetries of the square. We used as convention that entries in the table are of the form $r^i m^j$. Adopt the reverse convention, that is, write all entries as $m^j r^i$ and recompute the multiplication table. This is a good exercise if you are not yet comfortable with these multiplication tables!

Solution. We build a new multiplication table. (1) You can first fill up the first column and the first row (since multiplying by 1 does not change a symmetry). (2) Then using $r^4 = 1$, you can fill the 4×4 upper left corner involving only rotations, and (3) using that $m^2 = 1$, you can fill up the 5th row. (4) Now you can fill up the first 4 columns of rows 5, 6, 7 and 8, because all the terms that appear are of the form m and then a power of r:

	1	r	r^2	r^3	m	mr	mr^2	mr^3
1	1	r	r^2	r^3	m	mr	mr^2	mr^3
r	r	r^2	r^3	1				
r^2	r^2	r^3	1	r				
r^3	r^3	1	r	r^2				
m	m	mr	mr^2	mr^3	1	r	r^2	r^3
mr	mr	mr^2	mr^3	m				
mr^2	mr^2	mr^3	m	mr				
mr^3	mr^3	m	mr	mr^2				

We now use that $r^3m = mr$. Multiply both sides by r on the left, and r^{-1} on the right, to get

$$r(r^3m)r^{-1} = r(mr)r^{-1} \Rightarrow mr^{-1} = rm \Rightarrow mr^3 = rm.$$

Now knowing that $rm = mr^3$, by multiplying on the right by r, r^2 and r^3, we immediately get

$$rmr = mr^4 = m, \; rmr^2 = mr, \; rmr^3 = mr^2$$

and we can fill the second line of the table (in blue).

We now need to compute r^2m. We use that $rm = mr^3$, and multiply on the left by r:

$$r^2m = rmr^3 = (rm)r^3 = (mr^3)r^3 = mr^2$$

where we use a second time $rm = mr^3$. Now knowing that $r^2m = mr^2$, by multiplying on the right by r, r^2 and r^3, we immediately get

$$r^2mr = mr^3, \; r^2mr^2 = m, \; r^2mr^3 = mr$$

and we can fill the third line of the table (in blue). Do the same for the 4rth line!

	1	r	r^2	r^3	m	mr	mr^2	mr^3
1	1	r	r^2	r^3	m	mr	mr^2	mr^3
r	r	r^2	r^3	1	mr^3	m	mr	mr^2
r^2	r^2	r^3	1	r	mr^2	mr^3	m	mr
r^3	r^3	1	r	r^2	mr	mr^2	mr^3	m
m	m	mr	mr^2	mr^3	1	r	r^2	r^3
mr	mr	mr^2	mr^3	m				
mr^2	mr^2	mr^3	m	mr				
mr^3	mr^3	m	mr	mr^2				

To finish, we notice that (1) the 6th row is the second row multiplied by m on the left, (2) the 7th row is the third row multiplied by m on the left, and (3) that the 8th row is the 4rth row multiplied by m on the left:

	1	r	r^2	r^3	m	mr	mr^2	mr^3
1	1	r	r^2	r^3	m	mr	mr^2	mr^3
r	r	r^2	r^3	1	mr^3	m	mr	mr^2
r^2	r^2	r^3	1	r	mr^2	mr^3	m	mr
r^3	r^3	1	r	r^2	mr	mr^2	mr^3	m
m	m	mr	mr^2	mr^3	1	r	r^2	r^3
mr	mr	mr^2	mr^3	m	r^3	1	r	r^2
mr^2	mr^2	mr^3	m	mr	r^2	r^3	1	r
mr^3	mr^3	m	mr	mr^2	r	r^2	r^3	1

Once you are done, make sure every symmetry appears on every row of the table!

Exercises for Chapter 3

Before we give the solutions, it is useful to recall that to show that a set equipped with a binary operation is a group, we need to check the property of associativity. When the set is finite, it is always possible, though tedious, to check all possible triples. We will thus adopt the following: associativity of the addition and of the multiplication in $\mathbb{R}$ is considered as natural, thus we do not have to prove it. Based on it, it is then possible to prove associativity for addition and multiplication in $\mathbb{C}$. Also, associativity is natural for the composition of maps. It is always needed to mention associativity though, because you might encounter some non-associative map at some point of time!

Exercise 11. In Exercise 7, you determined the symmetries of an equilateral triangle, and computed the multiplication table of all its symmetries. Show that the symmetries of an equilateral triangle form a group.

1. Is it abelian or non-abelian?
2. What is the order of this group?
3. Compute the order of its elements.
4. Is this group cyclic?
5. Can you spot some of its subgroups? When you encounter such a question, it is enough to give an example of a subgroup which is not $\{1\}$, assuming that such a subgroup exists! If we want all the subgroups, then we will ask it explicitly!

Solution. For convenience, we recall the multiplication table:

	1	r	r^2	m_3	m_1	m_2
1	1	r	r^2	m_3	m_1	m_2
r	r	r^2	1	m_2	m_3	m_1
r^2	r^2	1	r	m_1	m_2	m_3
m_3	m_3	m_1	m_2	1	r	r^2
m_1	m_1	m_2	m_3	r^2	1	r
m_2	m_2	m_3	m_1	r	r^2	1

where m_1 is the reflection that goes through the lower left-hand corner of the triangle, m_2 is the reflection that goes through the lower right-hand corner of the triangle, m_3 is the vertical reflection, and r is the rotation of 120 degrees counter clockwise.

To show that the set G of symmetries of an equilateral triangle form a group, we need to check:

- G is closed under composition of symmetries, that is, combining two symmetries give another symmetry. There are several ways to argue that, for example: we know that this is the case for general isometries of the plane, so this is true in particular for symmetries of the equilateral triangle. In this case, since you also have a multiplication table, it can be seen from the table, since every element within the table is part of the group.

- Associativity holds, because composition of maps is associative.
- There is an identity element: 1=do-nothing.
- Every element is invertible: this was shown for every isometry of the plane, or can be shown from the multiplication table.

1. It is non-abelian (can be seen from the multiplication table which is not symmetric), or just by giving one counter-example, say $m_1 m_2 \neq m_2 m_1$ where m_1 is the mirror reflection going through the left corner, while m_2 is the mirror reflection going through the right corner.
2. The order of the group is its cardinality, it is thus 6.
3. 1=do-nothing has order 1, r and r^2 have order 3, the 3 other elements have order 2.
4. No, because no element has order 6.
5. Every element of order 2 generates a cyclic group of order 2. The rotation r generates a subgroup of order 3.

Exercise 12. Let $z = e^{2i\pi/3}$. Show that $\{1, z, z^2\}$ forms a group.

1. Is it abelian or non-abelian?
2. What is the order of this group?
3. Compute the order of its elements.
4. Is this group cyclic?
5. Can you spot some of its subgroups?

Solution. We show that $\{1, z, z^2\}$ forms a group.

- We have that $z^i z^j \in \{1, z, z^2\}$ for any $i, j \in \{0, 1, 2\}$ thus we have closure under multiplication.

- Associativity holds, it is inherited from the associativity of multiplication in $\mathbb{C}$.
- The identity element is 1.
- Every element is invertible: $z^{-i} \in \{1, z, z^2\}$ is the inverse of z^i for every $i \in \{0, 1, 2\}$.

1. It is abelian.
2. It is 3.
3. 1 is of order 1, z and z^2 are of order 3.
4. Yes, since it contains an element of order 3, which is the order of the group.
5. The only subgroups are the trivial subgroup $\{1\}$ and the group itself.

Exercise 13. Let X be a metric space equipped with a distance d.

1. Show that the set of bijective isometries of X (with respect to the distance d) forms a group denoted by G.
2. Let S be a subset of X. Define a symmetry f of S as a bijective isometry of X that maps S onto itself (that is $f(S) = S$). Show that the set of symmetries of S is a subgroup of G.

Note that as a corollary of this general result, we can deduce that the planar isometries form a group (where d is our usual distance), and the symmetries of the different shapes we saw are all subgroups!)

Solution. 1. Let G be the set of bijective isometries of X.

- We check that G is closed under composition: let f, g be two isometries, then

$$d(fg(x), fg(y)) = d(f(x), f(y)) = d(x, y)$$

  where the first equality holds since $g \in G$ and the second because $f \in G$. Thus the composition of two isometries is an isometry.
- Associativity holds, because composition of maps is associative.

- The identity is the do-nothing isometry.
- Every $f \in G$ is invertible because f is a bijection. But we still have to show that f^{-1} belongs to G.

  $$d(f^{-1}(x), f^{-1}(y)) = d(ff^{-1}(x), ff^{-1}(y)) = d(x, y)$$

  where the first equality holds because f is an isometry, and thus $f^{-1} \in G$.

2. To show that S is a subgroup, we need to check that it is a group under the same binary operation as G.

   - The composition of two symmetries is again a symmetry: indeed, a symmetry f by definition maps S into itself, that is $f(S) = S$, so the composition of two symmetries f, g will map S into itself: $gf(S) = g(S) = S$.
   - Associativity holds, because the composition of maps is associative.
   - 1=do-nothing is the identity.
   - We have to show that every symmetry has an inverse. Let $f \in S$ be a symmetry. We know it has an inverse f^{-1} in G, we have to check that this inverse is in S, that is, f^{-1} maps S to itself. Since $f(S) = S$, we have $f^{-1}f(S) = f^{-1}(S)$, that is $S = f^{-1}(S)$.

Exercise 14. Let G be a group. Show that right and left cancellation laws hold (with respect to the binary group operation), namely:

$$g_2 \cdot g_1 = g_3 \cdot g_1 \Rightarrow g_2 = g_3,$$

$$g_3 \cdot g_1 = g_3 \cdot g_2 \Rightarrow g_1 = g_2,$$

for any $g_1, g_2, g_3 \in G$.

Solution. We have

$$g_2 \cdot g_1 = g_3 \cdot g_1 \Rightarrow g_2 \cdot g_1 \cdot g_1^{-1} = g_3 \cdot g_1 \cdot g_1^{-1} \Rightarrow g_2 = g_3$$

using that every element is invertible, and that $g_1 \cdot g_1^{-1}$ is the identity element. Similarly

$$g_3 \cdot g_1 = g_3 \cdot g_2 \Rightarrow g_3^{-1} \cdot g_3 \cdot g_1 = g_3^{-1} \cdot g_3 \cdot g_2 \Rightarrow g_1 = g_2,$$

using again that every element is invertible, and that $g_3 \cdot g_3^{-1}$ is the identity element.

Exercise 15. Let G be an abelian group. Is the set

$$\{x \in G,\ x = x^{-1}\}$$

a subgroup of G? Justify your answer.

Exercise 16. Let G be a group, and let H be a subgroup of G. Consider the set

$$gH = \{gh,\ h \in H\}.$$

1. Show that $|gH| = |H|$.
2. Is thet set

   $$\{g \in G,\ gH = Hg\}$$

   a subgroup of G?

Exercise 17. Let G be a group, show that

$$(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1},$$

for every $g_1, g_2 \in G$. This is sometimes called the "shoes and socks property"!

Exercise 18. In a finite group G, every element has finite order. True or false? Justify your answer.

Exercise 19. This exercise is to practice Cayley tables.

1. Suppose that G is a group of order 2. Compute its Cayley table.

   Guided version.

   - Since G is of order 2, this means it has two elements, say $G = \{g_1, g_2\}$. Decide a binary law, say a binary law that is written multiplicatively.
   - Now use the definition of group to identify that one of the two elements must be an identity element 1. Then write the Cayley table.
   - Once you have written all the elements in the table, make sure that this table is indeed that of group! (namely make sure that you used the fact that every element is invertible).

2. Suppose that G is a group of order 3. Compute its Cayley table.

Solution.

1. If G has order 2, then we can write $G = \{g_1, g_2\}$. We suppose that the binary law is written multiplicatively. We know that the identity must be there, so we may assume that $g_1 = 1$ is the identity element. We now write the table:

	1	g_2
1	1	g_2
g_2	g_2	g_2^2

   but for this table to be a Cayley table of a group, we still need to see what happens with g_2^2. It must be an element of the group as well by closure. Now we know that g_2 must be invertible, which means that $g_2^2 = 1$.

2. We repeat the same for a group of order 3. Suppose that $G = \{1, g_2, g_3\}$ since one element must be the identity element. We get

	1	g_2	g_3
1	1	g_2	g_3
g_2	g_2		
g_3	g_3		

   Now using the closure property, $g_2 g_3$ must be an element of the group. It cannot be that $g_2 g_3 = g_2$ or g_3 (use the fact that g_2 and g_3 are invertible to see that), thus $g_2 g_3 = 1$, and by the same argument $g_3 g_2 = 1$. Thus

	1	g_2	g_3
1	1	g_2	g_3
g_2	g_2		1
g_3	g_3	1	

   which shows that $g_2^2 = g_3$, and $g_3^2 = g_2$, and we are done.

Exercise 20. Consider the set $M_n(\mathbb{R})$ of $n \times n$ matrices with coefficients in $\mathbb{R}$. For this exercise, you may assume that matrix addition and multiplication is associative.

1. Show that $M_n(\mathbb{R})$ is a group under addition.

2. Explain why $M_n(\mathbb{R})$ is not a group under multiplication.

3. Let $GL_n(\mathbb{R})$ be the subset of $M_n(\mathbb{R})$ consisting of all invertible matrices. Show that $GL_n(\mathbb{R})$ is a multiplicative group. ($GL_n(\mathbb{R})$ is called a *General Linear group*).

4. Let $SL_n(\mathbb{R})$ be the subset of $GL_n(\mathbb{R})$ consisting of all matrices with determinant 1. Show that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. ($SL_n(\mathbb{R})$ is called a *Special Linear group*).

5. Explain whether $SL_n(\mathbb{R})$ is a subgroup of $M_n(\mathbb{R})$

Solution.

1. Identity: The zero matrix is the identity element.
   Associativity is ok by assumption (alternatively, it is inherited by associativity of addition of complex numbers).
   Inverse of (A_{ij}) is $(-A_{ij})$.
   Closure: $(A_{ij}) + (B_{ij}) = C_{ij}$ with coefficient $C_{ij} = A_{ij} + B_{ij}$.

2. The zero matrix does not have a multiplicative inverse.

3. Identity: the identity matrix I_n.
   Associativity is ok by assumption.
   Inverse: by definition, all matrices in $GL_n(\mathbb{C})$ are invertible.
   Closure: Multiplying two invertible matrices gives another invertible matrix: $(AB)^{-1} = B^{-1}A^{-1}$.

4. Identity : $I_n \in SL_n(\mathbb{C})$, since certainly $\det(I_n) = 1$.
   Inverse: If $\det(A) = 1$, then $\det(A^{-1}) = 1/\det(A) = 1$, so the set contains inverses.
   Closure: if $\det(A) = \det(B) = 1$, then $\det(AB) = \det(A)\det(B) = 1$.

5. No, it is not, since $M_n(\mathbb{C})$ is an additive group, while $SL_n(\mathbb{C})$ is not closed under addition: $det(I_n + I_n) \neq 1$.

Exercises for Chapter 4

Exercise 21. We consider the set $\mathbb{C}$ of complex numbers.

1. Is $\mathbb{C}$ a group with respect to addition?

2. Is $\mathbb{C}$ a group with respect to multiplication?

3. In the case where $\mathbb{C}$ is a group, what is its order?

4. Can you spot some of its subgroups?

Solution.

1. Yes it is. The sum of two complex numbers is a complex number. Addition is associative. The identity element is 0, and every element x has an inverse $-x$, since $x - x = 0$.

2. No it is not, since 0 is not invertible. Indeed, the identity element is now 1, but there is no complex number y such that $y \cdot 0 = 1$. However, if you remove 0, then $\mathbb{C}$ without zero becomes a group! The product of two complex numbers is again a complex number, multiplication is associative, and every non-zero element x has an inverse x^{-1} since $x \cdot x^{-1} = 1$.

3. It is infinite.

4. So we need to look at $(\mathbb{C}, +)$. For example, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ are subgroups, all with identity element 0, and for x an inverse given by $-x$. Associativity is inherited from $\mathbb{C}$, and the closure under addition is clear. Also the even integers form a subgroup, since the sum of two even integers is even, the identity element is still 0, and $2y$ has for inverse $-2y$. If one consider $(\mathbb{C}\backslash\{0\}, \cdot)$, we similarly have $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{Q}\backslash\{0\}, \cdot)$, but $\mathbb{Z}$ does not work, since apart ± 1, integers are not invertible for multiplication. In that case, nth roots of unity are also a subgroup of $(\mathbb{C}\backslash\{0\}, \cdot)$.

Exercise 22. Alice and Bob have decided to use Caesar's cipher, however they think it is too easy to break. Thus they propose to use an affine cipher instead, that is

$$e_K(x) = k_1 x + k_2 \mod 26,\ K = (k_1, k_2).$$

Alice chooses $K = (7, 13)$, while Bob opts for $K = (13, 7)$. Which cipher do you think will be the best? Or are they both equally good?

Solution. The best cipher is that of Alice. Indeed

$$e_K(x) = 7x + 13 \mod 26$$

can be deciphered using

$$d_K(y) = 15y + 13 \mod 26$$

since

$$d_K(e_K(x)) = 15(7x+13)+13 = 15\cdot 7x+15\cdot 13+13 \equiv x+26 \equiv x \mod 26.$$

Now for the cipher of Bob, we have

$$e_K(x) = 13x+7 \mod 26$$

and 13 is not invertible modulo 26. Thus to decipher, we get

$$d_K(y) = \alpha y + \beta,$$

for some α, β, and

$$d_K(e_K(x)) = \alpha(13x+7)+\beta = \alpha\cdot 13x + 7\alpha + \beta.$$

Now we must solve $13\alpha x = x$ to find x, that is $x(13\alpha - 1) = 0$ and there is no α satistfying this equation.

Exercise 23. Show that the map $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$, $x \mapsto \exp(x)$ is a group homomorphism.

Solution. First we notice that $(\mathbb{R}, +)$ and $(\mathbb{R}\backslash\{0\}, \cdot)$ are both well-defined groups. Now we have to check the property of group homomorphism, namely

$$f(x+y) = f(x)f(y).$$

Now

$$f(x+y) = \exp(x+y) = \exp(x)\exp(y) = f(x)f(y).$$

Exercise 24. Show that a group homomorphism between two groups G and H always maps the identity element 1_G to the identity element 1_H.

Solution. You can show that using either additive or multiplication notation. In additive notation, we have that $f(a+b) = f(a) + f(b)$ thus take $a = 0$, which gives

$$f(0+b) = f(0)+f(b) \Rightarrow f(b) = f(0)+f(b) \Rightarrow 0 = f(0)$$

because $f(b)$ is invertible. In multiplicative notation, we have that $f(ab) = f(a)f(b)$ thus take $a = 1$, which gives

$$f(1\cdot b) = f(1)f(b) \Rightarrow f(b) = f(1)f(b) \Rightarrow 1 = f(1)$$

because $f(b)$ is invertible.

Exercise 25. In this exercise, we study a bit the invertible integers modulo n.

1. Take $n = 5$, and compute the group of invertible integers modulo 5. What is the order of this group? Can you recognize it? (in other words, is this group isomorphic to one of the groups we have already classified?)

2. Take $n = 8$, and compute the group of invertible integers modulo 8. What is the order of this group? Can you recognize it? (in other words, is this group isomorphic to one of the

   groups we have already classified?)

Solution.

1. The integers invertible modulo 5 are those coprime to 5, that is $\{1, 2, 3, 4\}$, so the order of the group is 4. We notice that 2 for example has order 4, since $2^4 = 16 \equiv 1 \mod 5$, thus this is a cyclic group of order 4, and since we know there is a unique cyclic group of order 4 up to isomorphism, we can also say this is "the" cyclic group of order 4.

2. The integers invertible modulo 8 are those coprime to 8, that is $\{1, 3, 5, 7\}$, so the order of the group is also 4. However, $3^2 \equiv 1 \mod 8$, $5^2 \equiv 1 \mod 8$ and $7^2 \equiv 1 \mod 8$, thus it cannot be cyclic. In fact, every element has order 2 but for the identity, so it follows easily that this group is isomorphic to the Klein group, that is the group of isometries of the rectange. To show formally the group isomorphism, one can define a map $f{:}\{1, 3, 5, 7\} \to \{1, r, m, rm\}$ where r is a rotation, m is a mirror reflection, as defined in the notes, such that

   $$f(1) = 1,\ f(3) = r,\ f(5) = m,\ f(7) = rm.$$

   We can check that $f(3 \cdot 5) = f(7) = rm = f(3)f(5)$ and similarly for all the pairs. In fact, any map that sends an element of order 2 to an element of order 2 will do!

Exercise 26. Let f be a group homomorphism $f : G \to H$ where G and H are two groups. Show that

$$f(g^{-1}) = f(g)^{-1}.$$

Solution. We have already seen that a group homomorphism is mapping the identity of G to the identity of H. To show the above property, we need to understand what it means. It means that it maps the inverse of g to the inverse of $f(g)$. Now we have by definition of group homomorphism that

$$f(g^{-1}g) = f(g^{-1})f(g),$$

and

$$1_H = f(1_G) = f(g^{-1}g) = f(g^{-1})f(g)$$

where we have added that f maps the identity of G to the identity of H. From this we can read what is written:

$$1_H = f(g^{-1})f(g)$$

which means that $f(g^{-1})$ is the inverse (we have checked only on the left) of $f(g)$, that is $f(g^{-1}) = f(g)^{-1}$. To complete the proof, we actually also need to check that $f(g)f(g^{-1}) = 1$, which can be done by replacing $g^{-1}g$ by gg^{-1} in the first equation, and derive everything again accordingly.

We have seen a few examples of group homomorphisms, or even group isomorphisms. You can take these examples and easily check for yourself that it works!

Exercise 27. Consider the group $(\mathbb{Z}, +)$ of integers under addition. Let H be a subgroup of $\mathbb{Z}$.

1. Show that H is of infinite order.
2. Use the Euclidean division algorithm to show that H is generated by a single element.
3. Find a subset of $\mathbb{Z}$ which forms a multiplicative group.

Here is a guided version of this exercise. Please try to do the normal version first!

1. Recall first what the order of a group is, to understand what it means for H to be of infinite order. Once this is clear, you need to use one of the properties of a group! If you cannot see which one, try each of them (can you cite the 4 of them?) and see which one will help you!

2. This one is more difficult. You will need to use a trick, namely use the minimality of some element...In every subgroup of $\mathbb{Z}$, there is a smallest positive integer (pay attention to the word"subgroup" here, this does not hold for a subset!).
3. To have a multiplicative group (that is a group with respect to multiplication), you need to define a set, and make sure this set together with multiplication satisfies the usual 4 properties of a group!

Solution.

1. Let $h \in H$ be an element other than the identity element. Then all multiples of h are contained in H by closure. It will follow that H is infinite once we show that all the multiples of h are distinct. To that end, suppose to the contrary that $mh = nh$. Then $(m-n)h = 0$, but that implies that $m = n$, since we assumed that h is not identity.
2. Let m be the smallest integer contained in H. We claim that any other element of H is a multiple of m. To that end, consider $h \in H$. For the sake of contradiction suppose h is not a multiple of m. Using the Euclidean Division Algorithm, we have $h = mq + r$, $r < m$. But then $r = h - mq \in H$, and r is smaller than m, contradicting the minimality of m in H.
3. Elements of a multiplicative group must have a multiplicative inverse. The only invertible integers are $\{\pm 1\}$, which form a group under multiplication.

Exercise 28. When we define a map on equivalence classes, the first thing we must check is that the map is *well defined*, that is, the map is independent of the choice of the representative of the equivalence class. In this exercise we give an example of a map which is *not well defined.*

Recall the parity map $sgn : \mathbb{Z} \to \mathbb{Z}/2$

$$sgn(2k+1) \mapsto 1$$

$$sgn(2k) \mapsto 0$$

Let $\mathbb{Z}/5\mathbb{Z}$ be the group of integers modulo 5. Let us attempt to define the map $sgn : \bar{a} \mapsto \overline{sgn(a)}$. Show that sgn is not well-defined on $\mathbb{Z}/5\mathbb{Z}$.

Solution. $sgn(\bar{1}) = sgn(1) = 1$ while $sgn(\bar{6}) = sgn(6) = 0$. But $\bar{1} = \bar{6}$, so their image should be the same. Hence the map sgn is not well-defined.

Exercises for Chapter 5

Exercise 29. Let G be a group and let H be a subgroup of G. Let gH be a coset of H. When is gH a subgroup of G?

Solution. If $g = 1$, we see that $gH = H$ and thus clearly H is a subgroup of G. In fact, if $g \in H$ (this includes $g = 1$ in particular), we have that $gH = H$. Indeed, $gH \subseteq H$, because every element of gH is of the form gh with g and h in H, and since H is a subgroup of G, it must be that $gh \in H$. Conversely, $H \subseteq gH$, since every element h in H can be written as $h = gh'$ with $h' = g^{-1}h$. We have thus shown that if $g \in H$, then $gH = H$ and thus gH is a subgroup. Now if g is not in H, gH cannot be a subgroup, because 1 does not belong to gH. Indeed, if 1 were to be in gH, then that means that there is an element $h \in H$ such that $gh = 1$, which means that g is the inverse of h, but the inverse of h belongs to H, while we know that this is not the case for g!

Exercise 30. As a corollary of Lagrange Theorem, we saw that the order of an element of a group G divides $|G|$. Now assume that d is an arbitrary divisor of $|G|$. Is there an element g in G with order d?

Solution. In general the answer is no. There are many counter-examples. For example, $|G|$ itself always divides $|G|$, but there exists an element of order $|G|$ only when the group is cyclic!

Exercise 31. Take as group G any group of order 50. Does it contain an element of order 7?

Solution. We have that $|G| = 50$. We know by Lagrange Theorem that the order of an element of G has to divide 50. Since 7 does not divide 50, there cannot be an element of order 7.

Exercise 32. Take as group G the Klein group of symmetries of the rectangle. Choose a subgroup H of G, write G as a partition of cosets of H, and check that the statement of Lagrange Theorem holds.

Solution. We can write the Klein group as $G = \{1, m, r, rm\}$. A subgroup is for example $H = \{1, m\}$ (or $\{1, r\}$, or $\{1, rm\}$). We have that

$$G = H \cup rH = \{1, m\} \cup \{r, rm\}.$$

The number of cosets of H is called the index of H in G, given by $[G : H] = 2$. The size of every coset is 2, and indeed

$$|G| = [G : H]|H| = 2 \cdot 2 = 4.$$

Exercise 33. This exercise looks at Lagrange Theorem in the case of an infinite group. Take as group $G = \mathbb{R}$ and as subgroup $H = \mathbb{Z}$. Compute the cosets of H and check that the cosets of H indeed partition G. Also check that the statement of Lagrange Theorem holds.

Solution. If $G = \mathbb{R}$, and $H = \mathbb{Z}$, cosets of $\mathbb{Z}$ are of the form $x + \mathbb{Z}$, $x \in \mathbb{R}$. Thus

$$\mathbb{R} = \bigcup_{0 \leq x < 1} (x + \mathbb{Z})$$

and $|\mathbb{R}| = |\mathbb{Z}| = \infty$.

Exercises for Chapter 6

Exercise 34. Show that any planar isometry of $\mathbb{R}^2$ is a product of at most 3 reflections.

Solution. We know from Theorem 2 that any planar isometry is either

a) A rotation about a point in the plane

b) A pure translation

c) A reflection about a line in the plane

d) A reflection about a line in the plane and a translation along the same line (glide reflection).

We consider each case.

a) A rotation about a point is a composition of two reflections about axes that meet at the fixed point (center of the rotation).

b) We saw that if we have two reflections of the form

$$\varphi_1 : z \to e^{i\theta_1}\bar{z} + \beta_1, \varphi_2 : z \to e^{i\theta_1}\bar{z} + \beta_2,$$

$$\varphi_2 \circ \varphi_1(z) = z + \underbrace{\overline{\beta_1} e^{i\theta} + \beta_2}_{\text{a translation vector}} .$$

This shows that the composition of two glide reflections gives a translation, and in fact any translation can be obtained in that way.

Now we want to express a translation in terms of two pure reflections. This means we need to consider extra constraints on β_1, β_2 in terms of θ_1, θ_2. To that end, recall that a glide reflection $e^{i\theta}\bar{z} + \beta$ is a pure reflection (that is, a reflection of order 2) whenever either $\beta = 0$ or the vector β is perpendicular to the reflection axis $\{e^{i\theta/2}x \mid x \in \mathbb{R}\}$. So, in particular, for choices $\beta_1 = 0$, $\beta_2 = w$ and $\theta/2 = arg(w) + \pi/2$, the glide reflections $\varphi_1(z) = e^{i\theta}\bar{z}$, $\varphi_2(z) = e^{i\theta}\bar{z} + w$ are in fact pure reflections whose composition $\varphi_2 \circ \varphi_1 = z + \overline{\beta_1}e^{i\theta} + \beta_2 = z + w$ corresponds to translation by w.

Geometrically, translation by w corresponds to reflection across the line P, followed by reflection across line $(P + w/2)$, where P is the line through the origin perpendicular to vector w, $(P + w/2)$ is the shift of P by $w/2$.

c) A reflection is a composition of a single reflection (itself!)

d) A glide reflection is a composition of a reflection and a translation (which is a composition of two reflections). As we have seen any composition of two reflections is always a rotation or a translation. A reflection cannot be a glide reflection since it does not have fixed point.

Exercise 35. Look at the pictures on the wiki (available on edventure), and find the symmetry group of the different images shown.

Exercises for Chapter 7

Exercise 36. Let σ be a permutation on 5 elements given by $\sigma = (15243)$. Compute sign(σ) (that is, the parity of the permutation).

Solution. This permutation sends 12345 to 54132, thus first we need to switch 1 and 5. $(15) : 12345 \mapsto 52341$. Now the first element is at the right place, but the second element should 4, not 2, thus we exchange 4 and 2.

$(24)(15) : 12345 \mapsto 54321$. We continue and exchange 1 and 3: $(13)(24)(15) : 12345 \mapsto 54123$. Finally, we exchange 2 and 3, to get $(23)(13)(24)(15) : 12345 \mapsto 54132$. Thus $\text{sign}(54132) = (-1)^4 = 1$.

Exercise 37.

1. Show that any permutation of the form $(i\ j\ k)$ is always contained in the alternating group A_n, $n \geq 3$.
2. Deduce that A_n is a non-abelian group for $n \geq 4$.

Solution.

1. Any permutation of the form $(i\,j\,k)$ can be written as $(i\,j)(j\,k)$, thus it is an even permutation, which belongs to A_n ($n \geq 3$ is needed to have 3 elements to permute).
2. It is enough to notice that $(1\ 2\ 3)$ and $(1\ 2\ 4)$ do not commute, since they are always contained in A_n, for $n \geq 4$.

Exercise 38. Let $H = \{\sigma \in S_5 \mid \sigma(1) = 1,\ \sigma(3) = 3\}$. Is H a subgroup of S_5?

Solution. We have that H is a subset of S_5 and thus it inherits associativity of composition from S_5. The identity (=do-nothing) permutation belongs to H. Let σ_1, σ_2 be two permutations in H. We have that

$$\sigma_1(\sigma_2(1)) = \sigma_1(1) = 1,\ \sigma_1(\sigma_2(3)) = \sigma_1(3) = 3$$

thus $\sigma_1\sigma_2 \in H$. Finally, we have to check that every element in H has an inverse in H. Let $\sigma \in H$, then

$$\sigma^{-1}(1) = \sigma^{-1}(\sigma(1)) = 1,\ \sigma^{-1}(1) = \sigma^{-1}(\sigma(3)) = 3$$

which shows that H is indeed a subgroup.

Exercise 39. In the lecture, we gave the main steps to show that the group D_6 cannot be isomorphic to the group A_4, though both of them are of order 12 and non-abelian. This exercise is about filling some of the missing details.

- Check that $(1\ 2)(3\ 4)$ is indeed of order 2.
- Check that $(1\ 2\ 3)$ is indeed of order 3.
- By looking at the possible orders of elements of D_6, prove that A_4 and D_6 cannot be isomorphic.

Solution.

- We have to check that $(12)(34)(12)(34) = ()$. We have

  $$(12)(34)(12)(34) : 1234 \mapsto 1243 \mapsto 2143 \mapsto 2134 \mapsto 1234.$$

  In fact, we can observe that what happens is that the two permutations are affecting disjoint subsets of indices, thus since we do (12) twice, and (34) twice, we get back the identity permutation.

- We compute (123)(123)(123):

  $$(123)(123)(123) : 123 \mapsto 231 \mapsto 312 \mapsto 123.$$

  In fact, every permutation is a shift of the 3 elements, and doing 3 shifts gives back the identity.

- D_6 contains a rotation r which is of order 6. We can check that no element of A_4 has order 6 (they are of order 2 and 3 only, the list of the elements and their order can be found in the lecture slide). Now if there were a group isomorphism f from D_6 to A_4, then $f(r)$ should be an element of order 6 in A_4, since

  $$f(r)^6 = f(r^6) = f(1) = 1$$

  and if there were a $k < 6$ such that $f(r)^k = 1$, then $f(r^k) = 1$, a contradiction. But there is no element of order 6 in A_4.

Exercises for Chapter 8

Exercise 40.

- Let G be the Klein group. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Identify this subgroup.

- Let G be the cyclic group C_4. Cayley's Theorem says that it is isomorphic to a subgroup of S_4. Identify this subgroup.

Solution.

- Let us write the multiplication table of the Klein group.

	1	g_1	g_2	g_3
1	1	g_1	g_2	g_3
g_1	g_1	1	g_3	g_2
g_2	g_2	g_3	1	g_1
g_3	g_3	g_2	g_1	1

We now interpret this table in terms of permutations. Let us label the elements of the group: $1 \to 1$, $g_1 \to 2$, $g_2 \to 3$, $g_3 \to 4$. The first row is then 1234, thus $1234 \to 1234$, the second row is 2143, thus $1234 \to 2143$, the third row is 3412 thus $1234 \to 3412$, finally the fourth row is 4321, thus $1234 \to 4321$. In cycle notation, this gives

$$(),\ (12)(34),\ (13)(24),\ (14)(23).$$

- Let us write the multiplication table of C_4.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

We now interpret this table in terms of permutations. The first row is 0123, thus $0123 \to 0123$, the second row is 1230, thus $0123 \to 1230$, the third row is 2301 thus $0123 \to 2301$, finally the fourth row is 3012, thus $0123 \to 3012$. In cycle notation, this gives

$$(),\ (0123),\ (02)(13),\ (0321)$$

but since we usually look at permutations on the elements $\{1, ..., n\}$, we rewrite these permutations as

$$(),\ (1234),\ (13)(24),\ (1432).$$

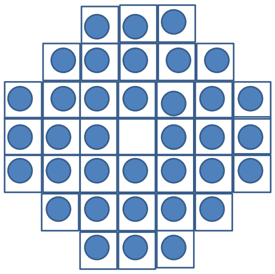
Exercise 41. Show that any rearrangement of pieces in the 15-puzzle starting from the standard configuration (pieces are ordered from 1 to 15, with the 16th position empty) which brings the empty space back to its original position must be an even permutation of the other 15 pieces.

Solution. We can view the overall puzzle as a permutation π in S_{15}, since the empty space returns to its original position. We can repeat the proof we did in the lecture, by replacing (14 15) by π. Namely

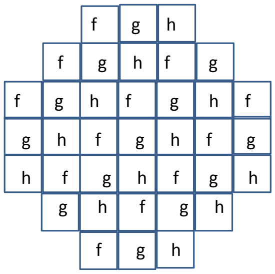
$$\pi = (a_n\ 16)(a_{n-1}\ 16)\cdots(a_2\ 16)(a_1\ 16).$$

Now the left hand side is an even permutation in S_{16} since the blank space 16 is moved an even number of positions (because 16 returns to its original location, it has to move up and down, as well as right and left, an equal number of times). The parity of a permutation in S_{15} is the same as its parity when viewed as a permutation in S_{16}, so π is an even permutation of the pieces 1,2,...,15.

Exercise 42. Has this following puzzle a solution? The rule of the game is the same as the solitaire seen in class, and a win is a single marble in the middle of the board. If a win is a single marble anywhere in the board, is that any easier?



Solution. We can solve this puzzle the same way we did in the lecture, namely by labeling the board with the Klein group $G = \{1, f, g, h\}$ as follows: Now



		f	g	h		
	f	g	h	f	g	
f	g	h	f	g	h	f
g	h	f	g	h	f	g
h	f	g	h	f	g	h
	g	h	f	g	h	
		f	g	h		

the total value of this board without the middle marble is

$$(fgh)^{12} = 1.$$

Since the total value is invariant by a move, whenever we move a marble and remove another one, the total value stays 1. Since no label is 1, not only it is impossible to finish with one marble in the center, but it is also impossible to finish with one marble all together!

Exercises for Chapter 9

Exercise 43. Consider the Klein group $G = \{1, f, g, h\}$.

- What are all the possible subgroups of G?
- Compute all the possible quotient groups of G.

Solution.

- First of all, by Lagrange Theorem, we know that subgroups of G have possible orders 1,2 and 4.
  - If the order of a subgroup is 1, then the subgroup is $\{1\}$.
  - If the order of a subgroup is 4, then the subgroup is G.

  We are left with the case where a subgroup has order 2. It will necessarily have 1 as part of it. Then we are left with three possibilities:

  $$\{1, f\}, \{1, g\}, \{1, h\}.$$

  Thus the list of all possible subgroups of G is:

  $$\{1\}, \{1, f\}, \{1, g\}, \{1, h\}, G.$$

- To compute a quotient group of G, we need a subgroup H that satisfies $g + H = H + g$. Because G is abelian, every subgroup listed above satisfies this property, thus we get 5 possible quotient groups:

  $$G/\{1\}, G/\{1, f\}, G/\{1, g\}, G/\{1, h\}, G/G.$$

  Since $|G/\{1\}| = |G|$, this group is G itself. Since $|G/H| = 2$ for every subgroup of order 2, in this case we get C_2. Finally $|G/G| = 1$, thus $G/G \simeq \{1\}$.

Exercise 44. Consider the dihedral group D_4. What are all the possible quotient groups of D_4?

Solution. Recall that the group D_4 is given by

$$D_4 = \{r, m \mid r^4 = m^2 = 1,\ mr = r^{-1}m\} = \{1, r, r^2, r^3, m, rm, r^2m, r^3m\}.$$

There are two ways of solving this exercise. One way is to list all the possible subgroups, and then check those which are normal. Since this can be quite tedious when the size of the dihedral group grows, we give a more theoretical argument. Recall that we found one subgroup that yields a quotient group in the lecture.

- Let r be a rotation. Then

  $$(r^jm)r^i = r^j(mr^i) = r^j(r^{-i}m) = r^{-i}(r^jm).$$

  This shows that $gH = Hg$ for every $g \in D_4$ and $H = \langle r \rangle$.

- The same property will thus be true for every subgroup of H! Here there is only one subgroup of H which is not $\{1\}$ or H, namely $\{1, r^2\}$.

So we have exhausted all the choices where the subgroup we consider contains only rotations. What if it contains a term of the form r^im? (with i possibly 0). Note that $gH = Hg \iff gHg^{-1} = H$. Thus if H contains an element r^im, it must also contain $g(r^im)g^{-1}$ where $g = r^jm$ or $g = r^j$ is an element of D_4. All right, let us thus compute $g(r^im)g^{-1}$. If $i = 0$, then

$$(r^jm)m(r^jm)^{-1} = (r^jm)mm^{-1}r^{-j} = r^jmr^{-j} = r^{2j}m,$$

and

$$(r^j)m(r^j)^{-1} = r^{2j}m.$$

Now what is $r^{2j}m$? Well j can take any value from 0 to 3. While j goes from 0 to 3, what are the values taken by $2j$? They are $0, 2, 0, 2$! (Note that this is happening because 4 is even). If $i = 1$, we can redo the same computations with rm instead of m, namely:

$$(r^jm)rm(r^jm)^{-1} = r^jmrmm^{-1}r^{-j} = r^jmrr^{-j} = r^jr^{j-1}m = r^{2j-1}m$$

and

$$(r^j)rm(r^j)^{-1} = r^jrr^jm = r^{2j+1}m.$$

When j takes values from 0 to 3, both $2j-1$ and $2j+1$ take values 3,1,3,1. We can do the same computations for $r^i m$, where i is either even or odd. In summary, we have two cases: if we have $r^i m$ with i even, then $g(r^i m)g^{-1} = r^{2j}m$, while if we have $r^i m$ with i odd, then $g(r^i m)g^{-1} = r^{2j-1}m$.

- If i is even, we thus know that H contains not only $r^i m$ but also $r^{2j}m = \{m, r^2 m\}$. Thus H further contains r^2 and
$$H = \{1, m, r^2 m, r^2\}.$$
- If i is odd, we similarly know that H contains not only $r^i m$ but also $r^{2j-1}m = \{rm, r^3 m\}$. Thus H further contains $rmr^3 m = rr^{-3} = r^2$ and
$$H = \{1, rm, r^2, r^3 m\}.$$

This gives the following list of subgroups that will yield a quotient group:

$$\{1\}, \{1, r^2\}, \{1, r, r^2, r^3\}, \{1, m, r^2 m, r^2\}, \{1, rm, r^2, r^3 m\}, D_4.$$

The corresponding quotient groups are

$$D_4, D_4/\{1, r^2\}, D_4/\{1, r, r^2, r^3\} \simeq C_2, D_4/\{1, m, r^2 m, r^2\} \simeq C_2, D_4/\{1, rm, r^2, r^3 m\} \simeq C_2, \{1\}.$$

Note that $|D_4/\{1, r^2\}| = 4$, thus it could be either C_4 or the Klein group.

Exercise 45. Consider A the set of affine maps of $\mathbb{R}$, that is

$$A = \{f : x \mapsto ax + b,\ a \in \mathbb{R}^*,\ b \in \mathbb{R}\}.$$

1. Show that A is a group with respect to the composition of maps.
2. Let
$$N = \{g : x \mapsto x + b,\ b \in \mathbb{R}\}.$$
Show that the set of cosets of N forms a group.
3. Show that the quotient group A/N is isomorphic to $\mathbb{R}^*$.

Solution. 1. Let $f, g \in A$. Then

$$(f \circ g)(x) = f(ax + b) = a'(ax + b) + b' = a'ax + a'b + b',$$

where $a'a \in \mathbb{R}^*$ thus the closure property is satisfied. The composition of maps is associative. The identity element is given by the identity map since

$$\mathrm{Id} \circ f = f \circ \mathrm{Id} = f.$$

Finally, we need to show that every $f \in A$ is invertible. Take $f^{-1}(x) = a^{-1}x - a^{-1}b$. Then

$$f^{-1} \circ f(x) = f^{-1}(ax+b) = a^{-1}(ax+b) - a^{-1}b = x.$$

2. We first notice that N is a subgroup of A (we need to check the usual things: closure, identity, inverse. Associativity is inherited.) Let $g \in N$ and let $f \in A$. We have to show that $fN = Nf$. Let us take $f(x) = ax + b \in A$ and $g(x) = x + b' \in N$. We have

   $$f \circ g(x) = f \circ (x + b') = a(x + b') + b = ax + ab' + b.$$

   On the other hand, define $g'(x) = x + ab'$, we have

   $$g' \circ f(x) = g'(ax + b) = ax + b + ab',$$

   and $f \circ g(x) = g' \circ f(x)$.

3. Elements of A/N are cosets of the form $fN = \{fg, g \in N\}$, with $f(x) = ax + b$, thus $fg(x) = f \circ g(x) = f(x + c) = ax + ac + b$, with $g(x) = x + c$. Also consider $f'(x) = a'x + b'$. Define the map

   $$\varphi : A/N \to \mathbb{R}^*,\ fN \mapsto a.$$

   It is a group homomorphism since

   $$\varphi(fNf'N) = \varphi(ff'N) = aa' = \varphi(f)\varphi(f'),$$

   where the 2nd equality follows from $ff'(x) = f(a'x+b') = a(a'x+b)+b = aa'x + ab + b$. To show that we have an isomorphism, we are left with 2 things to check

   - the map is a bijection (which is clear)
   - the map is well-defined, namely it does not depend on the choice of the coset representative f,

from which we conclude that

$$A/N \simeq \mathbb{R}^*.$$

Let us spend a minute to understand the interpretation of this result: when we look at all affine maps, and we take the quotient by those of the form $x + b$, that means that we consider as the same all maps whose coefficient in x is 1 no matter what is the constant term. Thus if the constant term does not matter, what is left that matters is the coefficient in x, that we denoted by a, which is why the quotient is in fact isomorphic to $\mathbb{R}^*$!

Exercises for Chapter 10

Exercise 46.

- Show that the complex numbers $\mathbb{C}$ form a vector space over the reals.
- Give a basis of $\mathbb{C}$ over the reals.
- In the lecture, we saw for $\mathbb{R}^2$ that we can obtain a new group, called a lattice, by keeping a basis of $\mathbb{R}^2$ but instead considering integer linear combinations instead of real linear combinations. What happens for $\mathbb{C}$ if we do the same thing? (namely consider integer linear combinations).

Solution.

- A complex number is of the form $a + ib$, thus it can be seen as a vector (a, b) over the reals. We need to check that vectors form an abelian group, which is clear: $\mathbf{0}$ is the identity element, (a, b) has an inverse given by $(-a, -b)$ for every vector (a, b), addition of vectors gives a vector, so closure is satisfied, as is associativity. The other properties for scalars are also clearly satisfied: distributivity of scalar multiplication with respect to vector and field (here the reals) addition, respect of scalar multiplication and identity element of scalar multiplication.
- We can write $\mathbb{C} = \{a + ib,\ a, b \in \mathbb{R}\} = \{(a, b),\ a, b \in \mathbb{R}\} = \{a(1, 0) + b(0, 1),\ a, b \in \mathbb{R}\}$. A natural basis is $\{(0, 1), (1, 0)\}$.
- By keeping the natural basis $\{(0, 1), (1, 0)\}$ we obtain the set

$$\{a + ib,\ a, b \in \mathbb{Z}\}$$

  which is usually denoted by $\mathbb{Z}[i]$. It is also an abelian group, it is isomorphic to $\mathbb{Z}^2$!

Exercise 47. Consider the set $\mathcal{M}_2(\mathbb{R})$ of 2×2 matrices with real coefficients.

1. Show that $\mathcal{M}_2(\mathbb{R})$ forms a vector space over the reals.
2. Deduce that it has an abelian group structure.
3. Give a basis of $\mathcal{M}_2(\mathbb{R})$ over the reals.
4. What happens for $\mathcal{M}_2(\mathbb{R})$ if we keep a basis over the reals and consider only integer linear combinations instead of real linear combinations? Do we also get a new group? If so, describe the group obtained.

Solution.

1. Matrices correpond to the vectors, we have to show they form an abelian group. The sum of two matrices is again a matrix (closure is satisfied), associativity holds. The identity element is the zero matrix. Let $M \in \mathcal{M}_2(\mathbb{R})$, then $-M$ is its inverse. The other properties for scalars are also clearly satisfied.

2. Once we have a vector space, we know that the vectors form an abelian group (here we actually showed the abelian group structure above).

3. A natural basis is the matrices E_{ij}, $i, j = 1, 2$, where E_{ij} denotes a matrix with zero everywhere but in the ith row, jth column, where there is a 1.

4. By keeping the natural basis $E_{11}, E_{12}, E_{21}, E_{22}$, we get the set of matrices $\mathcal{M}_2(\mathbb{Z})$. It is also an abelian group.

Exercises for Chapter 12

Exercise 48. Lagrange Theorem is likely to be the most important theorem of group theory, so let us revise it! Here is a bit of theory first:

- Can you remember what it states?
- The proof of Lagrange Theorem relies on a counting argument, based on the fact that cosets partition the group. Can you remember what cosets partition the group mean? If so, can you rederive the counting argument that proves Lagrange Theorem?

Now some more practice on how to use Lagrange Theorem!

- How many groups of order 5 do we have (up to isomorphism)?
- Consider the group of permutations S_5. Does S_5 contain a permutation of order 7?
- Suppose there exists an abelian group G of order 12 which contains a subgroup H of order 4. Show that the set of cosets of H forms a group. What is the order of G/H? Deduce what group G/H is.

Solution.

- It states that $[G:H]|H| = |G|$ where H is a subgroup of the group G, and $[G:H]$ denotes the number of cosets of H.
- Cosets partition the group mean that the union of cosets if the whole group, but the intersection of two cosets is either the whole coset or empty. Thus when we count how many elements we have in G, it is the same thing as counting how many cosets we have, times how many elements in each coset.
- Only 1. If the order is a prime, we know from Lagrange that the group has to be cyclic, thus up to isomorphism there is only the cyclic group of order 5.
- No, if there were, then 7 should divide $|S_5|$ by Lagrange, but $|S_5| = 5!$ which is not divisible by 7.
- The set of cosets always forms a group when G is abelian! The order of $|G/H|$ is $|G|/|H|$ by Lagrange, which is 3, thus G/H is the cyclic group of order 3.

Exercise 49. At the beginning of the class, we started by studying structure of geometric figures. We have seen shapes, and been asked what is their group of symmetries.

- Can you remember some of the shapes we studied, and what is the corresponding group of symmetries?
- Do you remember what are all the possible groups arising as symmetries of planar shapes?
- Let us do the reverse exercise: think of a symmetry group, and try to draw a figure that has this symmetry group.

Solution.

- For example, the rectangle with the Klein group, or the square with the dihedral group D_4.
- This is Leonardo Theorem: cyclic and dihedral groups.
- Hmm, that's thougher to give a solution to that!

Exercise 50. Let us remind a few things about permutations.

- What is the formal definition of a permutation?
- What is the parity of a permutation?
- Consider the permutation σ that maps:

  $$1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 5, 4 \mapsto 3, 5 \mapsto 6, 6 \mapsto 4, 7 \mapsto 7.$$

  Compute its parity.
- We have studied that the group of symmetries of a planar shape can be seen as a group of permutations. Do you remember how that works (either in general or on an example?)

Solution.

- It is a bijection.
- Write the permutation as a product of transpositions, count how many there are, and compute (-1) to the power the number of transpositions.
- This permutation can be written (12)(3564) or for example (12)(34)(36)(35) (there are many ways of writing it) so its parity is $(-1)^4 = 1$.

- We take the Cayley table of the group, and rewrite every row of the table as a permutation.

Exercise 51. Let us remember that planar isometries are either of type I: $H(z) = \alpha z + \beta,\ |\alpha| = 1$ or of type II: $H(z) = \alpha\bar{z} + \beta,\ |\alpha| = 1$.

- Show that the isometries of type I form a subgroup H of the group G of planar isometries.
- Show that G/H is a quotient group of order two.

Solution.

- (1) We need to check that the closure property is satisfied: take $H_1(z) = \alpha_1 z + \beta_1,\ |\alpha_1| = 1$, $H_2(z) = \alpha_2 z + \beta_2,\ |\alpha_2| = 1$, then

  $$H_1(H_2(z)) = H_1(\alpha_2 z + \beta_2) = \alpha_1(\alpha_2 z + \beta_2) + \beta_1$$

  showing that

  $$H_1(H_2(z)) = (\alpha_1\alpha_2)z + (\alpha_1\beta_2 + \beta_1)$$

  with $|\alpha_1\alpha_2| = 1$ (and similarly for $H_2(H_1(z))$). (2) Associativity of maps holds. (3) The identity map is of the right form (take $\beta = 0$ and $\alpha = 1$). (4) If $H(z) = \alpha z + \beta,\ |\alpha| = 1$, then $H^{-1}(z) = \alpha^{-1}z - \alpha^{-1}\beta$ Indeed

  $$H^{-1}H(z) = H^{-1}(\alpha z + \beta) = z + \alpha^{-1}\beta - \alpha^{-1}\beta = z.$$

- In order to show that we indeed have a quotient group G/H, where G is the group of planar isometries and H is the group of type I planar isometries, we need to show that H is a normal subgroup of G, namely, $gH = Hg$ for all $g \in G$. We observe that G is partitioned into two parts: type I and type II. The type I planar isometries form the subgroup H and the type II planar isometries form a left coset of H in G. Indeed, take any two type II planar isometries $f_1(z) = \alpha_1\bar{z} + \beta_1$ and $f_2(z) = \alpha_2\bar{z} + \beta_2$. We can show that $f_1H = f_2H$, or equivalently, $f_1 \circ f_2^{-1} \in H$:

  $$f_1 \circ f_2^{-1}(z) = f_1(f_2^{-1}(z)) = f_1(\frac{1}{\overline{\alpha_2}}\bar{z} - \frac{\overline{\beta_2}}{\overline{\alpha_2}}) = \alpha z + \beta,$$

  where α and β can be computed to confirm that $|\alpha| = 1$, verifying $f_1 \circ f_2^{-1} \in H$. A similar argument will give that the type II planar isometries form a right coset of H in G. Now we have obtained two partitions of G: $G = H \bigcup fH$ and $G = H \bigcup Hf$, where f is a type II planar isometry. Since $H = H$, we must have $fH = Hf$. We have shown that H is normal in G. (Note: this also shows that subgroups of index 2 are always normal.)

Finally, the quotient group is the cyclic group C_2 because the index of H in G is 2 and there is only one group of order 2.

Index

abelian, 45
alternating group, 165

Bézout's Identity, 79
basis, 215
bijective, 85

Caesar's cipher, 77
Cayley tables, 53
commutative, 45
complex conjugation, 5
congruent mod n, 71
coset, 103
cycle notation, 153
cyclic, 51

Dihedral group, 123
dihedral group, 141
distance, 5

equivalence class, 71
equivalence relation, 71
Euler Theorem, 119
Euler totient, 81

Fermat little theorem, 119
fixed point, 15
frieze, 229
frieze group, 237

glide, 135
group, 41
group isomorphism, 85

homomorphism, 85

identity, 41
identity map, 7
index, 111
injective, 85
inverse, 41
isomorphic, 85

Klein group, 129
Kleingroup, 115

Lagrange theorem, 109
lattice, 219

multiplication table, 29

normal subgroup, 197

one-to-one, 85
onto, 85
order of a group, 47
order of an element, 49

permutation, 149
planar isometry, 7
primitive, 83

quotient group, 199

reflection, 7
reflexive, 71

representative, 73
root of unity, 83
rotation, 7, 135

subgroup, 47
subspace, 215
surjective, 85
symmetric, 71
symmetric group, 149
symmetry, 25

transitive, 71
translation, 131
transposition, 161

vector space, 213

Bibliography

[1] http://plus.maths.org/content/power-groups.

[2] M. A. Armstrong. *Groups and Symmetry.* Springer.

[3] Keith Conrad. *Plane Isometries and the Complex Numbers.* www.math.uconn.edu/ kconrad/blurbs/grouptheory/isometrycpx.pdf.

[4] Keith Conrad. *Plane Isometries and the Complex Numbers.* http://www.math.uconn.edu/ kconrad/blurbs/grouptheory/15puzzle.pdf.

[5] David. W. Farmer. *Groups and Symmetry, a Guide to Discovering Mathematics.* American Mathematical Society.

[6] Joseph A. Gallian. *Contemporary Abstract Algebra.*

[7] Scott Kim. *Inversions.*